General Mode and Secret Mode Analysis by Web Browser

웹 브라우저 별 일반모드 및 시크릿모드 분석

발표자 아티fact체크!

CONTENTS

01 아티팩트?

- 아티팩트란?
- 사용 툴
- 상황 설명

02 Internet Explorer

- 브라우저 소개
- 일반모드
- 시크릿모드

03 Google Chrome

- 브라우저 소개
- 일반모드
- 시크릿모드

04 Firefox

- 브라우저 소개
- 일반모드
- 시크릿모드

05 Naver Whale

- 브라우저 소개
- 일반모드
- 시크릿모드

06 범죄 환경

- 범죄상황 설명
- 범죄상황 분석
- 결론

디지털 포렌식에서의 아티팩트(Artifact)?

: 운영체제나 애플리케이션을 사용하면서 생성되는 흔적

- **조사를 위해 주로 확인하는 정보**

Web History	사용자가 방문한 웹 사이트의 접속 정보로 편의를 위해 저장
Cache	웹 사이트 재접속 시 이미지나 정보들을 다시 다운로드 받지 않고 빠르게 로딩하기 위하여 사이트로부터 자동으로 받는 데이터
Cookie	웹 사이트에서 사용하는 사용자에 관한 데이터로 사용자의 하드 또는 서버에 저장
Download List	사용자가 의도적으로 선택하여 자신의 컴퓨터에 내려 받은 파일들에 대한 정보

① Volatility

사고 대응 및 멀웨어 분석을 위한 파이썬 기반 오픈소스 메모리 포렌식 툴

- 은닉되어 있는 프로세스를 조사
- 메모리 덤프 파일 분석 가능

② hxd

기본 메모리(RAM)의 원시 디스크 편집 및 수정 외에도 모든 크기의 파일을 처리하는 신중하게 설계된 빠른 16진수 편집기

- 기능: 검색 및 교체, 내보내기, 체크섬 / 다이제스트, 바이트 패턴 삽입, 파일 분쇄기, 파일 연결 또는 분할, 통계 등

③ Winhex

컴퓨터 포렌식 및 데이터 복구 소프트웨어, hex 편집기 및 디스크 편집기

- 핵심적인 범용 16진수 편집기
- 컴퓨터 포렌식, 데이터 복구, 저수준 데이터 처리 및 IT 보안 영역에서 유용
- 기능: 모든 종류의 파일을 검사 및 편집하고, 손상된 파일 시스템이 있는 하드 드라이브 또는 디지털 카메라 카드에서 삭제된 파일 또는 손실된 데이터를 복구

④ IE10Analyzer

WebCacheV01.dat 레코드 구문 분석 및 삭제 레코드 복구 툴

- WebCacheV01.dat : Internet Explorer 10, 11 및 Edge 브라우저에서 사용되는 History, Cache, Cookie 등의 로그를 관리하는 파일
- 삭제 된 기록을 복구할 수 있음
- InPrivate 브라우징 내용을 볼 수 있음

⑤ DB Browser for SQLite

오픈소스 소프트웨어로 SQLite 데이터베이스를 GUI 기반으로 편리하게 조작할 수 있도록 해 주는 툴

- 인덱스 생성, 삭제
- 데이터 조회, 업데이트, 삭제
- 데이터를 텍스트로 내보내기 또는 가져오기
- CSV 파일로 데이터 가져오기 및 내보내기

01

오후 8:14
2020-08-03

→

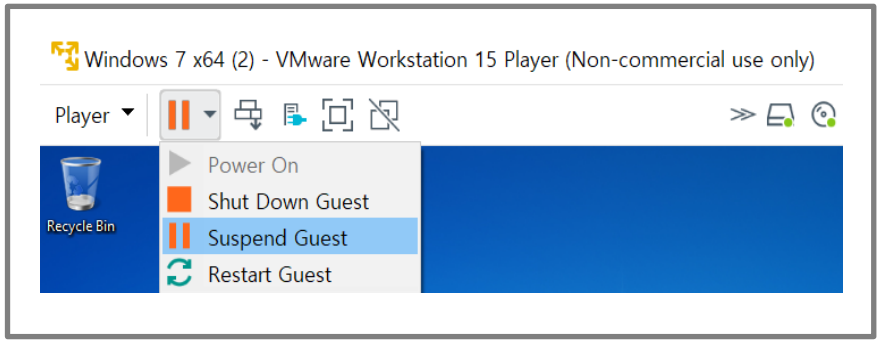
오후 8:45
2020-08-03

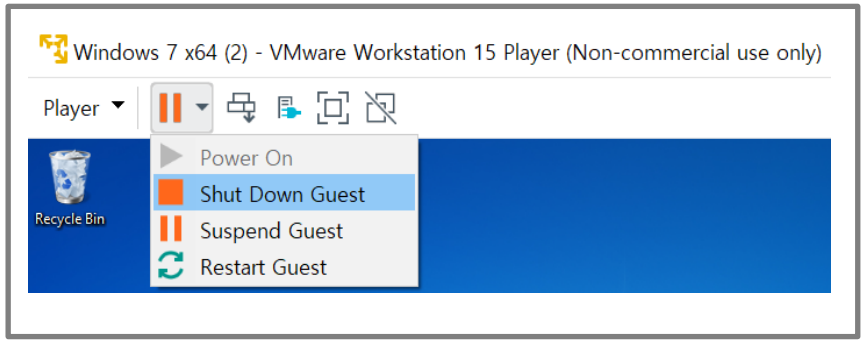
상황 1 : 〈shutdown 전〉

웹 브라우저 창 닫고 30분 후 바로 분석

상황 2 : 〈shutdown 후〉

웹 브라우저 창 닫고 30분 후, 전원 종료.
웹 브라우저 창을 켜고 분석





02

Internet Explorer

분석 – 조수경

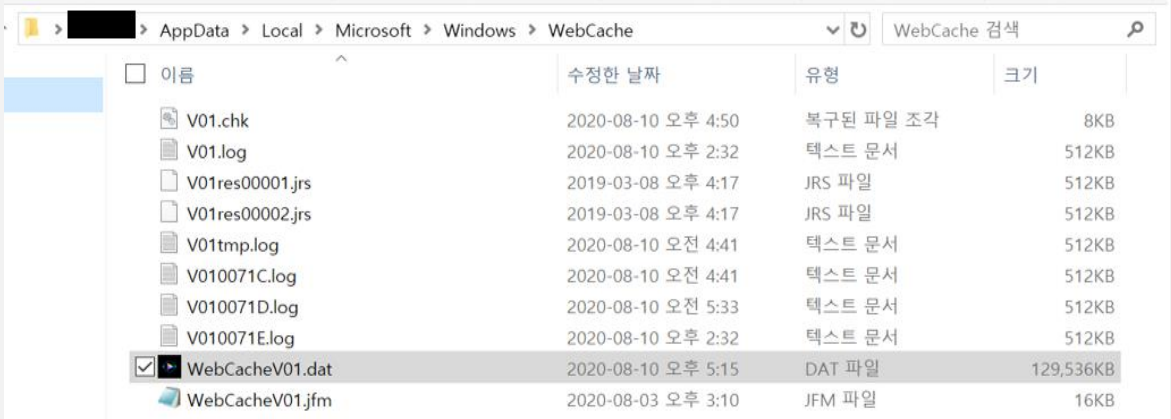
02

“ Internet Explorer ”

마이크로소프트사에서 개발
윈도우 운영체제를 설치할 때 자동 설치
범용적

02

WebCacheV01.dat



경로 : C:\Users\유저이름\AppData\Local\Microsoft\Windows\WebCache

History : History(L), History(M), MSHist01~
Cache: Content(L), Content(M)
Cookie: Cookies(L), Cookies(M)
Download: iedownload

일반모드 상황분석

〈shutdown 전〉

2980.dmp.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

https://www.bing.com/search?q=rambutan&FORM=IE8SRC&pc=EUPP_n+9

WIN-KGVN8EE98I9

Drive C: | pagefile.sys | $MFT

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
05B60B20	6E	6B	20	68	72	65	66	3D	22	2F	73	65	61	72	63	68	nk href="/search
05B60B30	3F	66	6F	72	6D	61	74	3D	72	73	73	26	61	6D	70	3B	?format=rss&
05B60B40	71	3D	72	61	6D	62	75	74	61	6E	26	61	6D	70	3B	71	q=rambutan&q

History(L)_Recovered

Visited: sue@https://www.bing.com/search?q=rambutan&f... rambutan - Bing

rambutan 검색 기록

메모리 덤프 파일
$MFT
History 파일

〈shutdown 후〉

860.dmp.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

http://www.bing.com/search?q=rambutan&FORM=IE8SRC&pc=EUPP_

\$MFT 5 days ago

Name	Ext.	Size	Created	Modified	Record change
.. = (Root directory)		8.2 KB	09-07-14d11:38:56	20-08-03d19:06:24	20-08-03d19:06

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0012E7B180	6E	6B	20	68	72	65	66	3D	22	2F	73	65	61	72	63	68	nk href="/search
0012E7B190	3F	66	6F	72	6D	61	74	3D	72	73	73	26	61	6D	70	3B	?format=rss&
0012E7B1A0	71	3D	72	61	6D	62	75	74	61	6E	26	61	6D	70	3B	46	q=rambutan&F

History(L)_Recovered | History(M)_Recovered

Url	WebPageInfo
Visited: sue@https://www.bing.com/search?q=rambutan&f...	rambutan - Bing

_Recovered | Content(L)_Recovered

Url

https://www.bing.com/search?q=rambutan&form=PRKRK...
https://www.bing.com/search?q=rambutan&form=PRKRK...

rambutan 검색 기록

메모리 덤프 파일
$MFT
History 파일 , Cache 파일

일반모드 상황분석

〈shutdown 전〉

2980.dmp.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

&url=https%3A%2F%2Fwww.eduwill.net%2FBasic%2Fglobal_main.asp&ref=https%3A%2F%2Fwww.bing.com

2980.dmp.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

search%3Fq%3Deduwill%26qs%3Dn%26form%3DQBRE%26sp%3D-1%26pq%3Deduwill%26sc%3D8-7%26s

History(L)_Recovered

Visited: sue@https://www.bing.com/search?q=eduwill&qs... eduwill - Bing

Visited: sue@https://img.eduwill.net/resources/eco/eco_l...

Visited: sue@https://www.eduwill.net/Basic/global_main.a... 에듀윌 - 꿈을 현실로 만드는 교육기업

www.eduwill.net 방문 기록

메모리 덤프 파일

History 파일

〈shutdown 후〉

860.dmp.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

www.eduwill.net/

https://www.eduwill.net/Img2/Common/Banner/111214/close_1.gif → 오늘 하루 안보기

Drive C: | pagefile.sys

\$MFT 5 days ago

Name	Ext.	Size	Created	Modified	Record change
.. = (Root directory)		8.2 KB	09-07-14d11:38:56	20-08-03d19:06:24	20-08-03d19:06

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
000D33FEF0	66	3D	22	68	74	74	70	73	3A	2F	2F	77	77	77	2E	65	f="https://www.e
000D33FF00	64	75	77	69	6C	6C	2E	6E	65	74	2F	42	61	73	69	63	duwill.net/Basic
000D33FF10	2F	67	6C	6F	62	61	6C	5F	6D	61	69	6E	2E	61	73	70	/global_main.asp
000D33FF20	22	20	68	3D	22	49	44	3D	53	45	52	50	2C	35	31	32	"h="ID=SERP,512

History(L)_Recovered History(M)_Recovered

Visited: sue@https://www.eduwill.net/Basic/global_main.a... 에듀윌 - 꿈을 현실로 만드는 교육기업

Cookies(L)_Recovered

Cookie:sue@eduwill.net/ BZS19C...

www.eduwill.net 방문 기록

메모리 덤프 파일
$MFT
History 파일 , Cookie 파일

일반모드 상황분석

〈shutdown 전〉

2980.dmp.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

C:₩Users₩sue₩Pictures₩img_award01.jpg
picture

img_award01.jpg 다운로드 기록

메모리 덤프 파일

〈shutdown 후〉

860.dmp.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

C:₩Users₩sue₩Pictures₩img_award01.jpg
picture

Drive C: | pagefile.sys
\$MFT 5 days ago

Name	Ext.	Size	Created	Modified	Record chang
.. = (Root directory)		8.2 KB	09-07-14d11:38:56	20-08-03d19:06:24	20-08-03d19:0

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
000BB129A0	00	08	00	00	00	00	1F	00	00	00	26	00	00	00	43	00	& C
000BB129B0	3A	00	5C	00	55	00	73	00	65	00	72	00	73	00	5C	00	: \ U s e r s \
000BB129C0	73	00	75	00	65	00	5C	00	50	00	69	00	63	00	74	00	s u e \ P i c t
000BB129D0	75	00	72	00	65	00	73	00	5C	00	69	00	6D	00	67	00	u r e s \ i m g
000BB129E0	5F	00	61	00	77	00	61	00	72	00	64	00	30	00	31	00	_ a w a r d 0 1
000BB129F0	2E	00	6A	00	70	00	67	00	00	00	25	00	00	00	03	00	. j p g %

History(M)_Recovered | feedplat(M)_Recovered | Content(L)_Recovered | Cookies(L)

0 Visited: sue@file:///C:/Users/sue/Pictures/img_award01.jpg

img_award01.jpg 다운로드 기록

메모리 덤프 파일
$MFT
History 파일

02

시크릿모드 상황분석

〈shutdown 전〉

〈shutdown 후〉

분석 결과 없음

jabuticaba 검색 기록

기록 없음

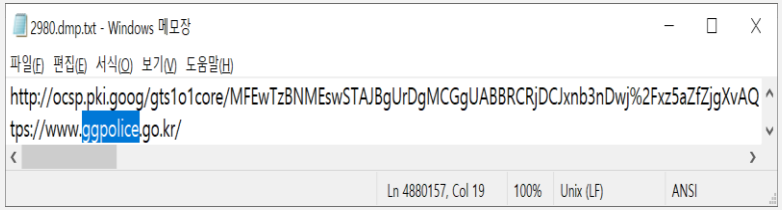
jabuticaba 검색 기록

기록 없음

02

시크릿모드 상황분석

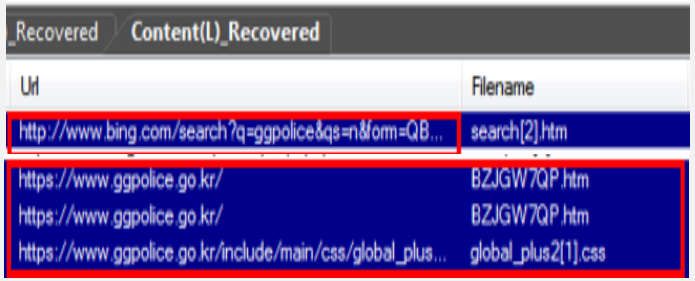
〈shutdown 전〉



www.ggpolice.go.kr 방문 기록

메모리 덤프 파일

〈shutdown 후〉



www.ggpolice.go.kr 방문 기록

메모리 덤프 파일

Cache 파일

02

시크릿모드 상황분석

〈shutdown 전〉

2980.dmp.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

₩Users₩sue₩Pictures₩main_fl_02.jpg

Main_fl_02.jpg 다운로드 기록

메모리 덤프 파일

〈shutdown 후〉

860.dmp.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

C:₩Users₩sue₩Pictures₩main_fl_02.jpg

picture

\$MFT 5 days ago

Name	Ext.	Size	Created	Modified	Record chang
.. = (Root directory)		8.2 KB	09-07-14d11:38:56	20-08-03d19:06:24	20-08-03d19:0

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
000264DA50	00	01	00	50	00	50	00	D0	07	01	00	00	02	01	00	10	P P Ð
000264DA60	0B	00	16	00	91	FA	67	00	E9	FF	DF	00	E1	E1	FF	00	'úg éÿß ááÿ
000264DA70	7C	68	DD	00	5A	00	F0	00	32	00	32	00	6D	61	69	6E	|hÝ Z ð 2 2 main
000264DA80	5F	66	6C	5F	30	32	2E	6A	70	67	00	2E	6B	72	00	00	_fl_02.jpg .kr

Main_fl_02.jpg 다운로드 기록

메모리 덤프 파일

03

Google Chrome

분석 – 안예린

“ Google Chrome ”

구글(Google)에서 개발하여 오픈 소스로 배포 중인 웹 브라우저이며 전 세계 웹 브라우저 점유율 69.35%.로 1위를 차지한다.

자바스크립트(javascript) 프로그래밍 언어와 함께 동적인 컨텐츠와 기능성 표현을 위한 HTML5의 웹 표준을 가장 우수하게 지원하는 웹 브라우저

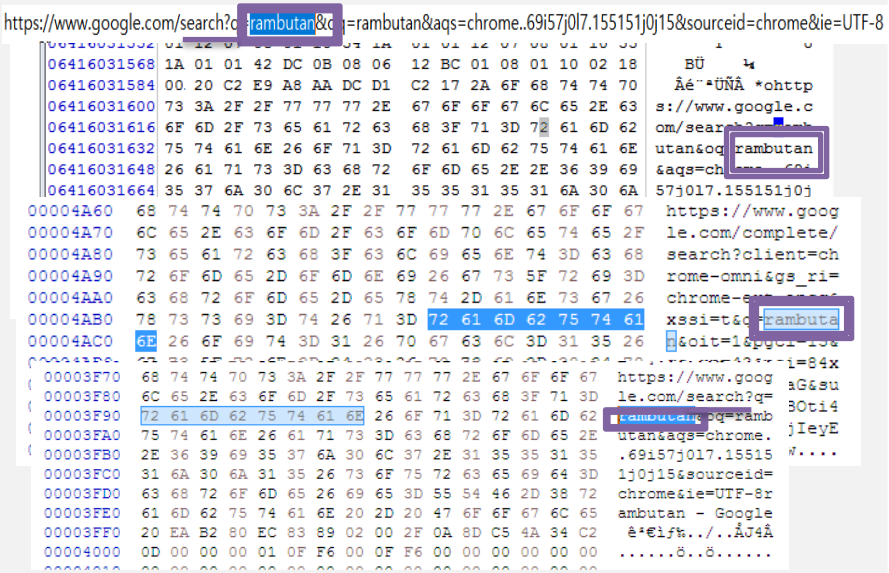
chrome

Cache	2020-08-15 오후 10:26	파일 폴더	
Cookies	2020-08-15 오후 10:26	파일	768KB
Cookies-journal	2020-08-15 오후 10:26	파일	0KB
CURRENT	2020-08-15 오후 7:50	파일	1KB
Current Session	2020-08-15 오후 9:15	파일	1KB
Current Tabs	2020-08-15 오후 6:28	파일	0KB
DownloadMetadata	2020-08-15 오후 2:49	파일	2KB
Favicons	2020-08-15 오후 10:26	파일	4,192KB
Favicons-journal	2020-08-15 오후 10:26	파일	0KB
Google Profile	2020-08-08 오후 1:59	아이콘	177KB
heavy_ad_intervention_opt_out	2020-06-04 오후 12:47	Data Base File	16KB
heavy_ad_intervention_opt_out.db-journal	2020-06-04 오후 12:47	DB-JOURNAL 파일	0KB
History	2020-08-15 오후 10:26	파일	5,216KB

경로 : C:\Users\USER\AppData\Local\Google\Chrome\UserData\Default
\cache, Cookie,history

History: download file list | **Cache**: data_0, data_1, data_2, data_3

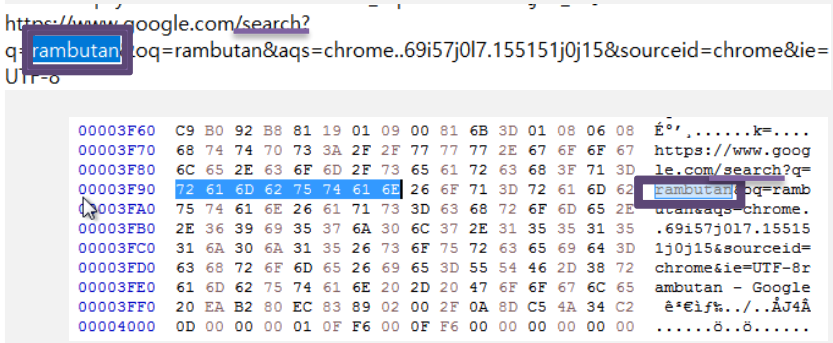
〈shoutdown 전〉



rambutan 검색 기록

cookie 파일을 제외하고 검색기록 확인

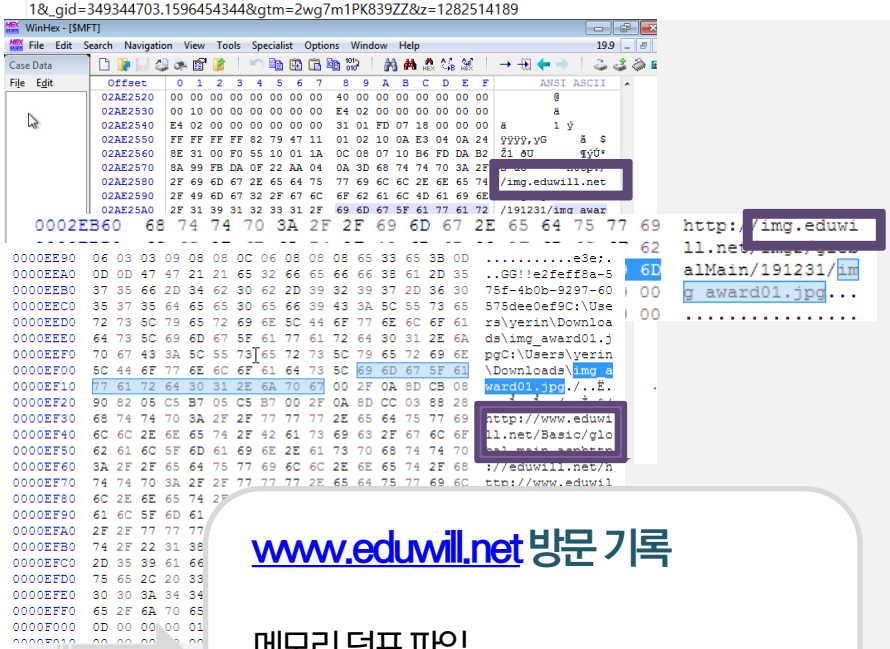
〈 shoutdown 후〉



rambutan 검색 기록

history , 메모리 덤프 파일 파일에서 검색기록 확인

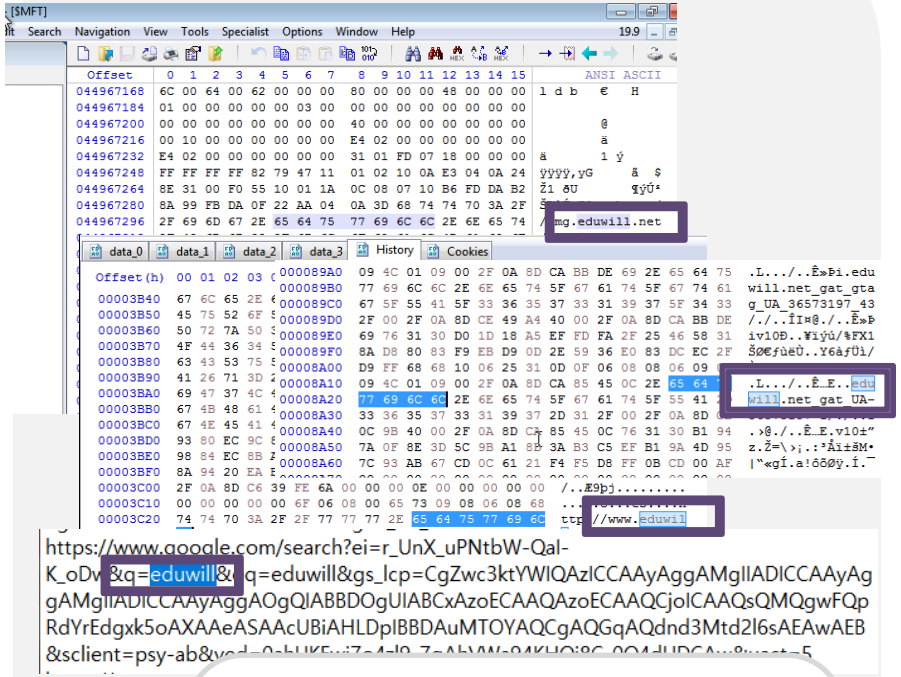
〈 shoutdown 전 〉



www.eduwill.net 방문 기록

메모리 덤프 파일
cache
$MFT
history

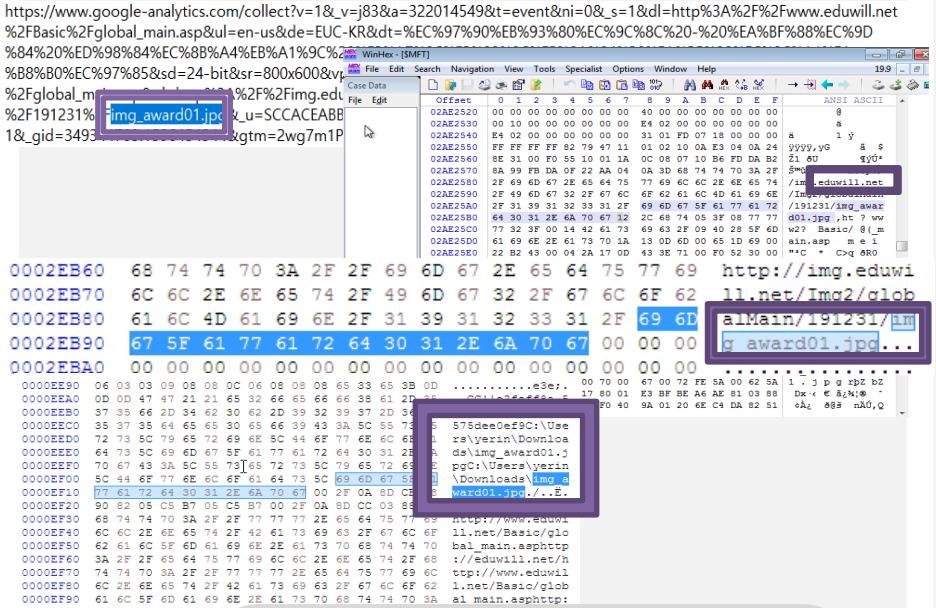
〈 shoutdown 후 〉



www.eduwill.net 방문 기록

메모리 덤프 파일
cookies
$MFT
history

〈 shoutdown 전 〉

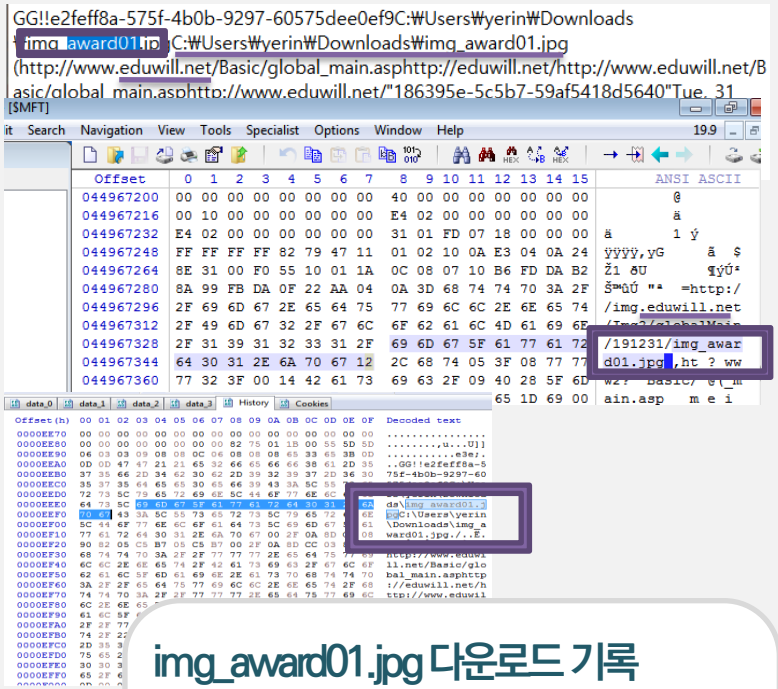


img_award01.jpg 다운로드 기록

메모리 덤프 파일, cache – 다운로드 받은 웹 사이트 , 파일 명

$MFT, history – 다운로드 받은 웹 사이트,다운로드 경로 , 파일 명

〈 shoutdown 후 〉



img_award01.jpg 다운로드 기록

$MFT – 파일 명, 다운로드 받은 웹 사이트

메모리 덤프 파일, history – 파일 명, 다운로드 받은 웹 사이트, 다운로드 경로

03

〈 shoutdown 전 〉

https://www.google.com/search?q=jabuticaba&q=jabuticaba&aqs=chrome..69i57.16427j0j1&sourceid=chrome&ie=UTF-8
Upgrade-Insecure-Requests: 1
https://www.google.com/search?ei=1_YnX_bjGJei-Qa83ZeoCw&q={searchTerms}
&oq=ggpoli&gs_lcp=CgZwc3ktYWIQAxgAMgIIADoECAAQQzoECAAQCjoECAAQHjoICAAQsQMQgwE6BQgAELEDUPfcBViOiwZgoJ8GaA
FwAHgEgAH6AYgB2RCSAQUwLjguNJgBAKABAaoBB2d3cy13aXqwAQDAAQE&sclient=psy-ab
UTF-8

jabuticaba 검색 기록

메모리 덤프 파일

〈 shoutdown 후 〉

jabuticaba 검색 기록

기록 없음

〈 shoutdown 전 〉

〈 shoutdown 후 〉

분석 결과 없음

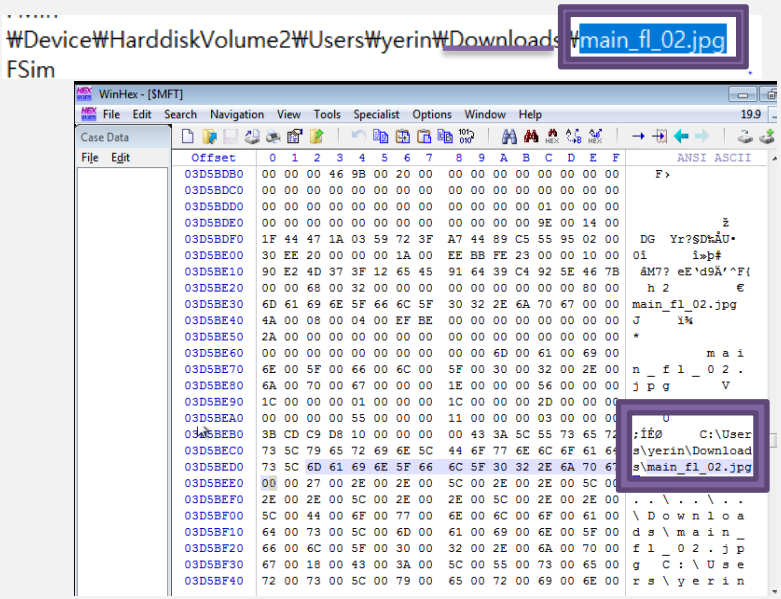
www.ggpolice.go.kr 방문 기록

기록 없음

www.ggpolice.go.kr 방문 기록

기록 없음

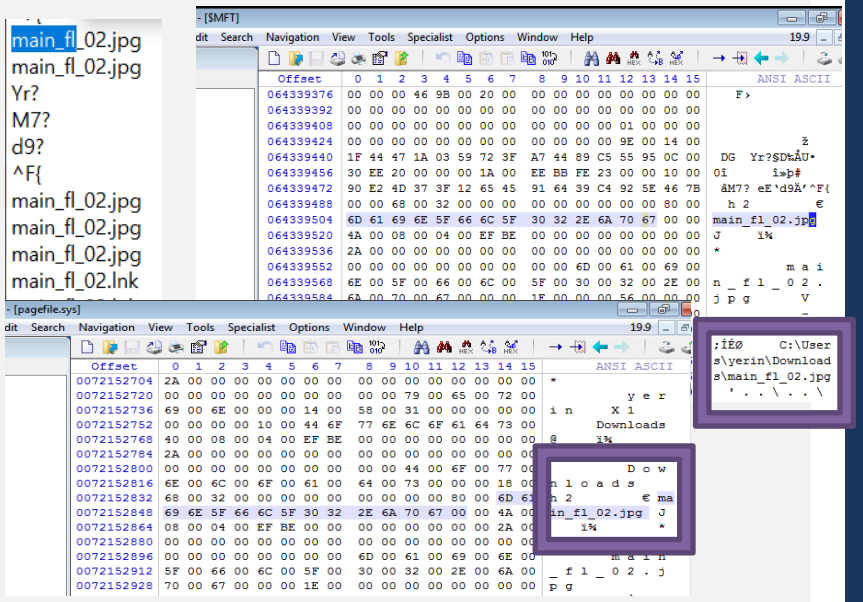
〈shoutdown 전〉



Main_fl_02.jpg 다운로드 기록

메모리 덤프 파일– 파일 명
$MFT–파일 명, 다운로드 경로

〈 shoutdown 후〉



Main_fl_02.jpg 다운로드 기록

메모리 덤프 파일, pagefile.sys – 파일 명
$MFT –다운로드 경로, 파일 명 확인

04

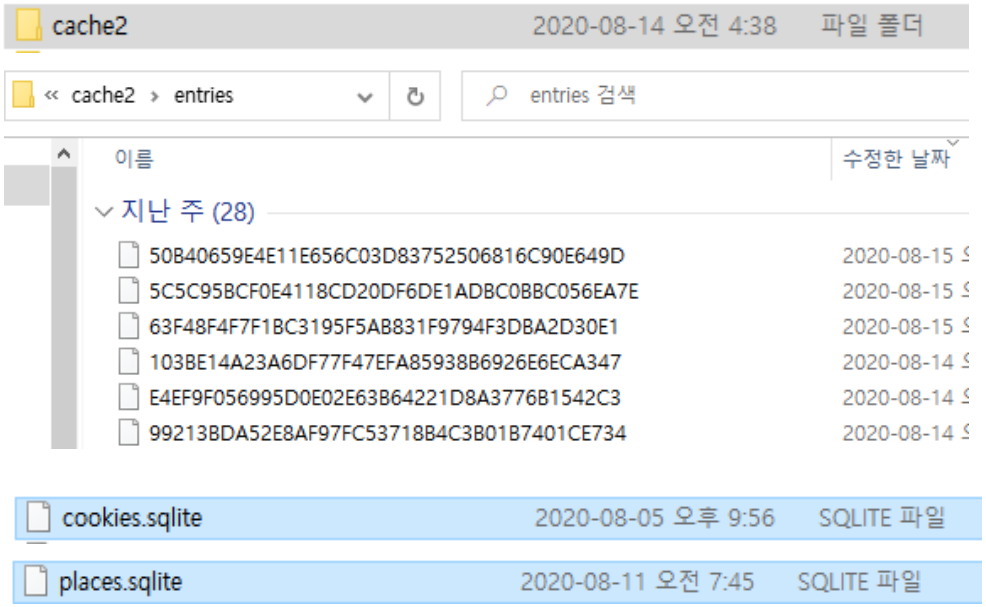
Firefox

분석 – 김수빈

04

“ Firefox ”

모질라에서 개발
전세계 웹 브라우저 시장 점유율 약 20% 차지
개인 정보 보호 및 보안에 두각



Cache: C:\Users\사용자 이름\AppData\Local\Mozilla\Firefox\Profiles\gu62w0z7.default-release\cache2\entries

Cookie: C:\Users\사용자 이름\AppData\Roaming\Mozilla\Firefox\Profiles\gu62w0z7.default-release\cookies.sqlite

History, Download: C:\Users\사용자이름\AppData\Roaming\Mozilla\Firefox\Profiles\gu62w0z7.default-release\places.sqlite

일반모드 상황분석

〈shutdown 전〉

4876 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
google
com
rambutan
NDsh
```

```
0001ACD0  9F EB 5F 28 CE 98 00 00 00 3C 00 00 00 00 3A 68  Ÿë_(Î˜...<....:h
0001ACE0  74 74 70 73 3A 2F 2F 77 77 77 2E 67 6F 6F 67 6C  ttps://www.googl
0001ACF0  65 2E 63 6F 6D 2F 73 65 61 72 63 68 3F 63 6C 69  e.com/search?cli
0001AD00  65 6E 74 3D 66 69 72 65 66 6F 78 2D 62 2D 64 26  ent=firefox-b-d&
0001AD10  71 3D 72 61 6D 62 75 74 61 6E 00 6E 65 63 6B 6F  q=rambutan.necko
```

```
4 00 77 77 77 2E 67 6F 6F  67 6C 65 2E 63 6F 6D 2F   www.google.com/
0 B4 3F F7 0F 3F 63 6C 69  65 6E 74 3D 66 69 72 65   ´?÷ ?client=fire
6 66 6F 78 2D 62 2D 64 26  71 3D 72 61 6D 62 75 74   fox-b-d&q=rambut
2 61 6E 58 1E 04 13 00 41  20 2D 20 47 45 00 7F 20   anX    A - GE
```

8 ... rambutan - Google 검색 moc.elgo

rambutan 검색 기록

메모리 덤프 파일
Cache 파일
$MFT
History 파일

〈shutdown 후〉

2984 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
moc.elgoog.www.d
bBvli_0NiDFc+
https://www.google.com/search?client=firefox-b-d&q=rambutanrambutan
moc.elgoog.www.
```

```
0001ACD0  9F EB 5F 28 CE 98 00 00 00 3C 00 00 00 00 3A 68  Ÿë_(Î˜...<....:h
0001ACE0  74 74 70 73 3A 2F 2F 77 77 77 2E 67 6F 6F 67 6C  ttps://www.googl
0001ACF0  65 2E 63 6F 6D 2F 73 65 61 72 63 68 3F 63 6C 69  e.com/search?cli
0001AD00  65 6E 74 3D 66 69 72 65 66 6F 78 2D 62 2D 64 26  ent=firefox-b-d&
0001AD10  71 3D 72 61 6D 62 75 74 61 6E 00 6E 65 63 6B 6F  q=rambutan.necko
```

```
4 00 77 77 77 2E 67 6F 6F  67 6C 65 2E 63 6F 6D 2F   www.google.com/
0 B4 3F F7 0F 3F 63 6C 69  65 6E 74 3D 66 69 72 65   ´?÷ ?client=fire
6 66 6F 78 2D 62 2D 64 26  71 3D 72 61 6D 62 75 74   fox-b-d&q=rambut
2 61 6E 58 1E 04 13 00 41  20 2D 20 47 45 00 7F 20   anX    A - GE
```

8 ... rambutan - Google 검색 moc.elgo

rambutan 검색 기록

메모리 덤프 파일
Cache 파일
$MFT
History 파일

일반모드 상황분석

〈shutdown 전〉

4876 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

ReferrerUrl=http://www.eduwill.net/Basic/global_main.asp

```
0002E9A0  00 00 00 00 3A 68 74 74 70 73 3A 2F 2F 77 77 77  ....:https://www
0002E9B0  2E 67 6F 6F 67 6C 65 2E 63 6F 6D 2F 73 65 61 72  .google.com/sear
0002E9C0  63 68 3F 63 6C 69 65 6E 74 3D 66 69 72 65 66 6F  ch?client=firefo
0002E9D0  78 2D 62 2D 64 26 65 69 3D 6D 4F 30 6E 58 2D 32  x-b-d&ei=m00nX-2
0002E9E0  39 48 4D 75 74 6F 41 53 6A 32 4A 62 34 42 41 26  9HMutoASj2Jb4BA&
0002E9F0  71 3D 65 64 75 77 69 6C 6C 26 6F 71 3D 65 64 75  q=eduwill&oq=edu
0002EA00  77 69 6C 6C 26 67 73 5F 6C 63 70 3D 43 67 5A 77  will&gs_lcp=CgZw
```

9	...	eduwill - Google 검색	moc.elgo
10		에듀윌 - 꿈을 현실로 만드는 교육기업	ten.lliwud
11		에듀윌 - 꿈을 현실로 만드는 교육기업	ten.lliwud

www.eduwill.net 방문 기록

메모리 덤프 파일
Cache 파일
History 파일

〈shutdown 후〉

2984 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

{Hy
yCw
http://img.eduwill.net/Img2/globalMain/191231/img_award01.jpgimg_award01.jpgten.lliwude.gmi.

```
0002E9A0  00 00 00 00 3A 68 74 74 70 73 3A 2F 2F 77 77 77  ....:https://www
0002E9B0  2E 67 6F 6F 67 6C 65 2E 63 6F 6D 2F 73 65 61 72  .google.com/sear
0002E9C0  63 68 3F 63 6C 69 65 6E 74 3D 66 69 72 65 66 6F  ch?client=firefo
0002E9D0  78 2D 62 2D 64 26 65 69 3D 6D 4F 30 6E 58 2D 32  x-b-d&ei=m00nX-2
0002E9E0  39 48 4D 75 74 6F 41 53 6A 32 4A 62 34 42 41 26  9HMutoASj2Jb4BA&
0002E9F0  71 3D 65 64 75 77 69 6C 6C 26 6F 71 3D 65 64 75  q=eduwill&oq=edu
0002EA00  77 69 6C 6C 26 67 73 5F 6C 63 70 3D 43 67 5A 77  will&gs_lcp=CgZw
```

```
6  5F 70 76 30 2E 77 77 77  2E 65 64 75 77 69 6C 6C  _pv0.www.eduwill
2  2E 6E 65 74 2F 5F 31 F0  4B 00 05 AC 8E EA 4C 71  .net/_1ðK  ¬ŽêLq
```

9	...	eduwill - Google 검색	moc.elgo
10		에듀윌 - 꿈을 현실로 만드는 교육기업	ten.lliwud
11		에듀윌 - 꿈을 현실로 만드는 교육기업	ten.lliwud

www.eduwill.net 방문 기록

메모리 덤프 파일
Cache 파일
History 파일
$MFT

일반모드 상황분석

〈shutdown 전〉

4876 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

C:₩Users₩ ₩Desktop₩img_award01.jpg

```
66 69 6C 65 3A 2F 2F 2F  43 3A 2F 55 73 65 72 73   file:///C:/Users
2F 73 75 62 69 6E 2F 44  65 73 6B 74 6F 70 2F 69   /subin/Desktop/i
6D 67 5F 61 77 61 72 64  30 31 2E 6A 70 67 04 03   mg_award01.jpg
```

```
0007FFC0  66 69 6C 65 3A 2F 2F 2F 43 3A 2F 55 73 65 72 73   file:///C:/Users
0007FFD0  2F 73 75 62 69 6E 2F 44 65 73 6B 74 6F 70 2F 69   /subin/Desktop/i
0007FFE0  6D 67 5F 61 77 61 72 64 30 31 2E 6A 70 67 04 03   mg_award01.jpg..
```

12 .. img_award01.jpg

img_award01.jpg 다운로드 기록

메모리 덤프 파일
Pagefile.sys
History 파일

〈shutdown 후〉

2984 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

C:₩Users₩subin₩Desktop₩img_award01.jpg

```
2 10 00 00 00 00 43 3A 5C  55 73 65 72 73 5C 73 75   C:\Users\su
8 62 69 6E 5C 44 65 73 6B  74 6F 70 5C 69 6D 67 5F   bin\Desktop\img_
4 61 77 61 72 64 30 31 2E  6A 70 67 00 00 26 00 2E   award01.jpg  & .
```

```
0007FFC0  66 69 6C 65 3A 2F 2F 2F 43 3A 2F 55 73 65 72 73   file:///C:/Users
0007FFD0  2F 73 75 62 69 6E 2F 44 65 73 6B 74 6F 70 2F 69   /subin/Desktop/i
0007FFE0  6D 67 5F 61 77 61 72 64 30 31 2E 6A 70 67 04 03   mg_award01.jpg..
```

12 .. img_award01.jpg

img_award01.jpg 다운로드 기록

메모리 덤프 파일
Pagefile.sys
History 파일

04

시크릿모드 상황분석

〈shutdown 전〉

〈shutdown 후〉

분석 결과 없음

jabuticaba 검색 기록

기록 없음

jabuticaba 검색 기록

기록 없음

04

시크릿모드 상황분석

〈shutdown 전〉

4876 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

ggpolice.go.kr
www.ggpolice.go.kr0

www.ggpolice.go.kr 방문 기록

메모리 덤프 파일

〈shutdown 후〉

www.ggpolice.go.kr 방문 기록

기록 없음

시크릿모드 상황분석

〈shutdown 전〉

4876 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

₩Users₩subin₩Desktop₩main_fl_02.jpg:Zone.Identifier

Main_fl_02.jpg 다운로드 기록

메모리 덤프 파일

〈shutdown 후〉

2984 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

₩Device₩HarddiskVolume2₩Users₩subin₩Desktop₩main_fl_02.jpg

```
7C 68 DD 00 5A 00 F0 00  32 00 32 00 6D 61 69 6E  |hÝ Z ð 2 2 main
5F 66 6C 5F 30 32 2E 6A  70 67 00 00 00 00 00 00  _fl_02.jpg
```

Main_fl_02.jpg 다운로드 기록

메모리 덤프 파일

Pagefile.sys

05

Naver Whale

분석 – 김성연

05

“ Naver Whale ”

네이버에서 5년동안 자체적으로 개발해 2017년 9월에 런칭한 브라우저
Chrominum 오픈소스를 기반으로 만들어져 크롬과 AppData가 유사

네이버에서 설명하는 시크릿모드는
방문기록, 쿠키, 자동완성, 임시파일에 관련한 내용은 저장하지 않으며,
다운로드 목록, 북마크, 아이디와 비밀번호 기록은 저장이 된다고 한다.

NAVER

whale

Chromium

Naver Whale
네이버웨일

네이버웨일의 AppData

이름	수정한 날짜
TransportSecurity	2020-06-01 오전 6:51
Cookies	2020-06-01 오전 6:51
Cookies-journal	2020-06-01 오전 6:51
Network Persistent State	2020-06-01 오전 6:31
Preferences	2020-06-01 오전 6:31
Favicons	2020-06-01 오전 6:30
Favicons-journal	2020-06-01 오전 6:30
History	2020-06-01 오전 6:30
History-journal	2020-06-01 오전 6:30
Network Action Predictor	2020-06-01 오전 6:30
README	2020-06-01 오전 5:40
Cache	2020-06-01 오전 6:30
Pepper Data	2020-06-01 오전 6:30

경로 : C:\Users\사용자명\AppData\Local\Naver\Naver Whale\UserData\Default

Cookies, History, Current Tabs, Favicons, Cache 등 중요 정보가 들어있다.

일반모드 상황분석

〈shutdown 전〉

https://search.naver.com/search.naver?ie=UTF-8&sm=whl_hty&query=rambutanrambutan :

History

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00003F70	ED	95	A9	EA	B2	80	EC	83	89	00	2F	0A	CE	31	1D	C3	[illegible]
00003F80	B1	30	7C	01	0A	00	81	1D	4F	09	08	06	08	0F	68	74	±0|.....O.....ht
00003F90	74	70	73	3A	2F	2F	73	65	61	72	63	68	2E	6E	61	76	tps://search.nav
00003FA0	65	72	2E	63	6F	6D	2F	73	65	61	72	63	68	2E	6E	61	er.com/search.na
00003FB0	76	65	72	3F	69	65	3D	55	54	46	2D	38	26	73	6D	3D	ver?ie=UTF-8&sm=
00003FC0	77	68	6C	5F	68	74	79	26	71	75	65	72	79	3D	72	61	whl_hty&query=ra
00003FD0	6D	62	75	74	61	6E	72	61	6D	62	75	74	61	6E	20	3A	mbutanrambutan :
00003FE0	20	EB	84	A4	EC	9D	B4	EB	B2	84	20	ED	86	B5	ED	95	[illegible]
00003FF0	A9	EA	B2	80	EC	83	89	00	2F	0A	CE	30	97	60	DB	30	[illegible]
00004000	0D	00	00	00	01	0F	F6	00	0F	F6	00	00	00	00	00	00	.....ö..ö.....

Drive C: pagefile.sys

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
0302522192	EC	8B	A4	EB	A1	9C	20	EB	A7	8C	EB	93	9C	EB	8A	94	[illegible]
0302522352	B1	30	7C	01	0A	00	81	1D	4F	09	08	06	08	0F	68	74	±0| O ht
0302522368	74	70	73	3A	2F	2F	73	65	61	72	63	68	2E	6E	61	76	tps://search.nav
0302522384	65	72	2E	63	6F	6D	2F	73	65	61	72	63	68	2E	6E	61	er.com/search.na
0302522400	76	65	72	3F	69	65	3D	55	54	46	2D	38	26	73	6D	3D	ver?ie=UTF-8&sm=
0302522416	77	68	6C	5F	68	74	79	26	71	75	65	72	79	3D	72	61	whl_hty&query=ra
0302522432	6D	62	75	74	61	6E	72	61	6D	62	75	74	61	6E	20	3A	mbutanrambutan :
0302522448	20	EB	84	A4	EC	9D	B4	EB	B2	84	20	ED	86	B5	ED	95	[illegible]

rambutan 검색 기록

메모리 덤프 파일

Current Session, Current Tabs, Network Action Predictor ,Favicons, History, data_1 Pagefile.sys

〈shutdown 후〉

5https://ac.search.naver.com/nx/ac?of=os&ie=UTF-8&sm=whl_hty&q=rambutan&oe=UTF-8 https://ac.search.naver.com/nx/ac?q_enc=UTF-8&r_format=json&r_enc=UTF-8&r_unicode=0&ans=2&frm=whale&q=rambutan

Last Session

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000D360	18	00	00	00	68	74	74	70	73	3A	2F	2F	73	65	61	72	....https://sear
0000D370	63	68	2E	6E	61	76	65	72	2E	63	6F	6D	05	00	00	02	ch.naver.com....
0000D380	00	00	00	00	00	00	00	00	02	00	00	00	48	00	00	00	.....H...
0000D390	68	74	74	70	73	3A	2F	2F	73	65	61	72	63	68	2E	6E	https://search.n
0000D3A0	61	76	65	72	2E	63	6F	6D	2F	73	65	61	72	63	68	2E	aver.com/search.
0000D3B0	6E	61	76	65	72	3F	69	65	3D	55	54	46	2D	38	26	73	naver?ie=UTF-8&s
0000D3C0	6D	3D	77	68	6C	5F	68	74	79	26	71	75	65	72	79	3D	m=whl_hty&query=
0000D3D0	72	61	6D	62	75	74	61	6E	00	00	00	00	DB	60	97	30	rambutan....Ü`—0
0000D3E0	CE	0A	2F	00	00	00	00	00	C8	00	00	00	02	00	00	00	Î./.....È.....

Last Tabs

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00005210	00	00	00	00	08	00	00	00	00	00	00	00	20	00	00	00	....
00005220	18	00	00	00	68	74	74	70	73	3A	2F	2F	73	65	61	72	....https://sear
00005230	63	68	2E	6E	61	76	65	72	2E	63	6F	6D	05	00	00	02	ch.naver.com....
00005240	00	00	00	00	00	00	00	00	02	00	00	00	48	00	00	00	.....H...
00005250	68	74	74	70	73	3A	2F	2F	73	65	61	72	63	68	2E	6E	https://search.n
00005260	61	76	65	72	2E	63	6F	6D	2F	73	65	61	72	63	68	2E	aver.com/search.
00005270	6E	61	76	65	72	3F	69	65	3D	55	54	46	2D	38	26	73	naver?ie=UTF-8&s
00005280	6D	3D	77	68	6C	5F	68	74	79	26	71	75	65	72	79	3D	m=whl_hty&query=
00005290	72	61	6D	62	75	74	61	6E	00	00	00	00	DB	60	97	30	rambutan....Ü`—0
000052A0	CE	0A	2F	00	00	00	00	00	C8	00	00	00	02	00	00	00	Î./.....È.....
000052B0	00	00	00	00	DB	60	97	30	CE	0A	2F	00	FF	FF	FF	FF	....Ü`—0Î./.ÿÿÿÿ

rambutan 검색 기록

메모리 덤프 파일

Favicons, Network Action Predictor, Last Tabs, Last Session, History, data_1

일반모드 상황분석

〈shutdown 전〉

```
,http://www.eduwill.net/Basic/global_main.asp
http://unisolated.invalid/",http://www.eduwill.net/Basic/global_main.asp*}http://www.eduwill.net/?
NaPm=ct%3Dkdj0f5fn%7Cci%3Dcheckout%7Ctr%3Dds%7Ctrx%3D%7Chk
%3Dd5341be63eb554e18969f50a921daeb973a537be0
"27f52a0-5c5b7-59af5418d5640"J
Tue, 31 Dec 2019 00:44:01 GMT
```

```
History
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
0001CBD0  00 00 00 00 00 00 30 03 65 01 68 74 74 70 3A 2F  ......0.e.http:/
0001CBE0  2F 77 77 77 2E 65 64 75 77 69 6C 6C 2E 6E 65 74  /www.eduwill.net
0001CBF0  2F 42 61 73 69 63 2F 67 6C 6F 62 61 6C 5F 6D 61  /Basic/global_ma
0001CC00  69 6E 2E 61 73 70 06 81 02 04 82 07 01 68 74 74  in.asp......htt
0001CC10  70 3A 2F 2F 77 77 77 2E 65 64 75 77 69 6C 6C 2E  p://www.eduwill.
0001CC20  6E 65 74 2F 3F 4E 61 50 6D 3D 63 74 25 33 44 6B  net/?NaPm=ct%3Dk
```

```
Drive C: $MFT
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
05BF4DE0  12 2C 68 74 74 70 3A 2F  2F 77 77 77 2E 65 64 75  ,http://www.edu
05BF4DF0  77 69 6C 6C 2E 6E 65 74  2F 42 61 73 69 63 05 00  will.net/Basic
05BF4E00  6C 6F 62 61 6C 5F 6D 61  69 6E 2E 61 73 70 1A 1A  lobal_main.asp
05BF4E10  68 74 74 70 3A 2F 2F 75  6E 69 73 6F 6C 61 74 65  http://unisolate
05BF4E20  64 2E 69 6E 76 61 6C 69  64 2F 22 2C 68 74 74 70  d.invalid/",http
05BF4E30  3A 2F 2F 77 77 77 2E 65  64 75 77 69 6C 6C 2E 6E  ://www.eduwill.n
05BF4E40  65 74 2F 42 61 73 69 63  2F 67 6C 6F 62 61 6C 5F  et/Basic/global_
05BF4E50  6D 61 69 6E 2E 61 73 70  2A 7D 68 74 74 70 3A 2F  main.asp*}http:/
05BF4E60  2F 77 77 77 2E 65 64 75  77 69 6C 6C 2E 6E 65 74  /www.eduwill.net
05BF4E70  2F 3F 4E 61 50 6D 3D 63  74 25 33 44 6B 64 6A 30  /?NaPm=ct%3Dkdj0
```

```
Drive C: pagefile.sys
Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   ANSI ASCII
0292966864 4E 6E 61 6D 65 73 70 61  63 65 2D 30 39 37 30 32  Nnamespace-09702
0292966880 37 62 35 5F 37 35 38 35  5F 34 30 31 37 5F 38 66  7b5_7585_4017_8f
0292966896 38 38 5F 64 35 64 63 61  63 33 33 37 64 32 34 2D  88_d5dcac337d24-
0292966912 68 74 74 70 3A 2F 2F 77  77 77 2E 65 64 75 77 69  http://www.eduwi
0292966928 6C 6C 2E 6E 65 74 2F 01  0F 00 00 00 00 00 00 01  ll.net/
```

www.eduwill.net 방문 기록

메모리 덤프 파일

Current Session, Current Tabs, Favicons, History, Network Action Predictor, Preference, data_1, data_2

$MFT, Pagefile.sys

〈shutdown 후〉

```
Fu1
Zhttps://inflow.pay.naver.com/rd?tr=ds&retUrl=http%3A%2F%2Fwww.eduwill.net
%2F&pType=P&no=&vcode=5nr37hTMbR0M2dOdVUu0tetK00noYyBp%2BcrYPeedB%2FnjHIz
%2FnNTTBh5lLw6JY5RmlLKJrKPrB7Df5oLJUfWSkQ%3D%3D
```

```
History
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
0001CBD0  00 00 00 00 00 00 30 03 65 01 68 74 74 70 3A 2F  ......0.e.http:/
0001CBE0  2F 77 77 77 2E 65 64 75 77 69 6C 6C 2E 6E 65 74  /www.eduwill.net
0001CBF0  2F 42 61 73 69 63 2F 67 6C 6F 62 61 6C 5F 6D 61  /Basic/global_ma
0001CC00  69 6E 2E 61 73 70 06 81 02 04 82 07 01 68 74 74  in.asp....,..htt
0001CC10  70 3A 2F 2F 77 77 77 2E 65 64 75 77 69 6C 6C 2E  p://www.eduwill.
0001CC20  6E 65 74 2F 3F 4E 61 50 6D 3D 63 74 25 33 44 6B  net/?NaPm=ct%3Dk
```

```
Drive C: $MFT
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
05BF4DE0  12 2C 68 74 74 70 3A 2F  2F 77 77 77 2E 65 64 75  ,http://www.edu
05BF4DF0  77 69 6C 6C 2E 6E 65 74  2F 42 61 73 69 63 05 00  will.net/Basic
05BF4E00  6C 6F 62 61 6C 5F 6D 61  69 6E 2E 61 73 70 1A 1A  lobal_main.asp
05BF4E10  68 74 74 70 3A 2F 2F 75  6E 69 73 6F 6C 61 74 65  http://unisolate
05BF4E20  64 2E 69 6E 76 61 6C 69  64 2F 22 2C 68 74 74 70  d.invalid/",http
05BF4E30  3A 2F 2F 77 77 77 2E 65  64 75 77 69 6C 6C 2E 6E  ://www.eduwill.n
05BF4E40  65 74 2F 42 61 73 69 63  2F 67 6C 6F 62 61 6C 5F  et/Basic/global_
05BF4E50  6D 61 69 6E 2E 61 73 70  2A 7D 68 74 74 70 3A 2F  main.asp*}http:/
05BF4E60  2F 77 77 77 2E 65 64 75  77 69 6C 6C 2E 6E 65 74  /www.eduwill.net
05BF4E70  2F 3F 4E 61 50 6D 3D 63  74 25 33 44 6B 64 6A 30  /?NaPm=ct%3Dkdj0
```

www.eduwill.net 방문 기록

메모리 덤프 파일

Last Session, Last Tabs, Favicons, History, Network Action Predictor, Preference, cookies, data_1, data_2

$MFT

일반모드 상황분석

〈shutdown 전〉

=http://img.eduwill.net/Img2/globalMain/191231/img_award01.jpg
₩Device₩HarddiskVolume2₩Users₩sungyeon₩Downloads₩836ea2b3-5785-44a0-a40b-af48347f660c.tmp
₩Device₩HarddiskVolume2₩Users₩sungyeon₩Downloads₩img_award01.jpg.crdownload
₩Device₩HarddiskVolume2₩Users₩sungyeon₩Downloads₩img_award01.jpg.crdownload
₩Device₩HarddiskVolume2₩Users₩sungyeon₩Downloads₩img_award01.jpg
ce₩
₩Windows₩System32₩shdocvw.dll

History

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000FFA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000FFB0	00	00	00	00	00	00	00	00	00	00	00	00	42	01	05	09	.....B...
0000FFC0	08	81	07	68	74	74	70	3A	2F	2F	69	6D	67	2E	65	64	...http://img.ed
0000FFD0	75	77	69	6C	6C	2E	6E	65	74	2F	49	6D	67	32	2F	67	uwill.net/Img2/g
0000FFE0	6C	6F	62	61	6C	4D	61	69	6E	2F	31	39	31	32	33	31	lobalMain/191231
0000FFF0	2F	69	6D	67	5F	61	77	61	72	64	30	31	2E	6A	70	67	/img_award01.jpg
00010000	0A	00	00	00	01	0F	FB	00	0F	FB	00	00	00	00	00	00	.....û..û.....

Drive C: $MFT

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
05BF4D90	0D	08	00	10	CD	DC	E2	DC	DA	EA	8B	94	A3	01	22	D8	Í0âÚÊ‹"£ "Ø
05BF4DA0	03	0A	3D	68	74	74	70	3A	2F	2F	69	6D	67	2E	65	64	=http://img.ed
05BF4DB0	75	77	69	6C	6C	2E	6E	65	74	2F	49	6D	67	32	2F	67	uwill.net/Img2/g
05BF4DC0	6C	6F	62	61	6C	4D	61	69	6E	2F	31	39	31	32	33	31	lobalMain/191231
05BF4DD0	2F	69	6D	67	5F	61	77	61	72	64	30	31	2E	6A	70	67	/img_award01.jpg
05BF4DE0	12	2C	68	74	74	70	3A	2F	2F	77	77	77	2E	65	64	75	,http://www.edu
05BF4DF0	77	69	6C	6C	2E	6E	65	74	2F	42	61	73	69	63	05	00	will.net/Basic
05BF4E00	6C	6F	62	61	6C	5F	6D	61	69	6E	2E	61	73	70	1A	1A	lobal_main.asp
05BF4E10	68	74	74	70	3A	2F	2F	75	6E	69	73	6F	6C	61	74	65	http://unisolate
05BF4E20	64	2E	69	6E	76	61	6C	69	64	2F	22	2C	68	74	74	70	d.invalid/",http
05BF4E30	3A	2F	2F	77	77	77	2E	65	64	75	77	69	6C	6C	2E	6E	://www.eduwill.n
05BF4E40	65	74	2F	42	61	73	69	63	2F	67	6C	6F	62	61	6C	5F	et/Basic/global_
05BF4E50	6D	61	69	6E	2E	61	73	70	2A	7D	68	74	74	70	3A	2F	main.asp*}http:/
05BF4E60	2F	77	77	77	2E	65	64	75	77	69	6C	6C	2E	6E	65	74	/www.eduwill.net
05BF4E70	2F	3F	4E	61	50	6D	3D	63	74	25	33	44	6B	64	6A	30	/?NaPm=ct%3Dkdj0

img_award01.jpg 다운로드 기록

메모리 덤프 파일
History, data_1
$MFT, Pagefile.sys

〈shutdown 후〉

Qhttp://pmp.eduwill.net/eduwillpmp/eduwill/flv/globalCommecial/20180102/global_3.mp4
https://clients1.google.com/tbproxy/af/query?
q=Chc2LjEuMTcxNS4xNDQyL2VulChHR0xMKRMZKXPUkjBGeTsjLYuQFJ8kly0_B2X5JCMtJATU3SQjLQKk8MA
kly0Axvv5JCMtSQfnrCQjLUybECIkFBMZflgfbipAjEgjLfKH6-kkly2BLy05JCMt4lpd-
CQjLSuDPvokly3iARyEJCMtcH8XeyQUExkrl_yuz-e-
iCMtkWGVTiQUExlmqdp8uGQy2CMtuFYaLCQjLQp40JokFA==
7http://img.eduwill.net/Img2/globalMain/191231/img_award01.jpg
ohttp://img.eduwill.net/Img2/globalMain/title_area.gif

data_1

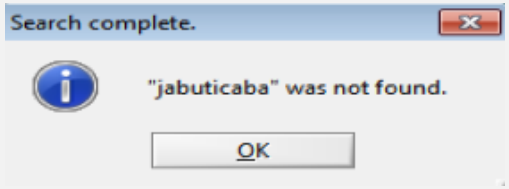
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00026E50	00	00	00	00	00	00	00	00	00	00	00	00	68	87	D0	37	.....h‡Ð7
00026E60	68	74	74	70	3A	2F	2F	69	6D	67	2E	65	64	75	77	69	http://img.eduwi
00026E70	6C	6C	2E	6E	65	74	2F	49	6D	67	32	2F	67	6C	6F	62	ll.net/Img2/glob
00026E80	61	6C	4D	61	69	6E	2F	31	39	31	32	33	31	2F	69	6D	alMain/191231/im
00026E90	67	5F	61	77	61	72	64	30	31	2E	6A	70	67	00	00	00	g_award01.jpg...

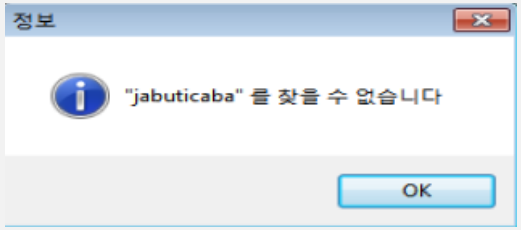
img_award01.jpg 다운로드 기록

메모리 덤프 파일
History, data_1

시크릿모드 상황분석

〈shutdown 전〉

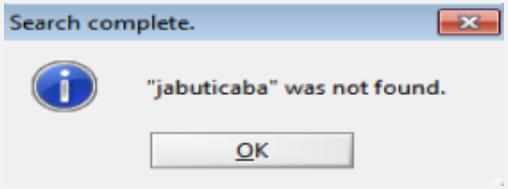


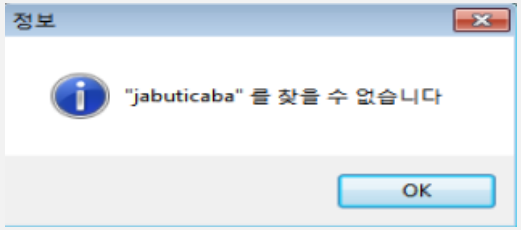


jabuticaba 검색 기록

기록 없음

〈shutdown 후〉





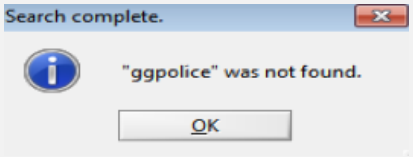
jabuticaba 검색 기록

기록 없음

시크릿모드 상황분석

〈shutdown 전〉

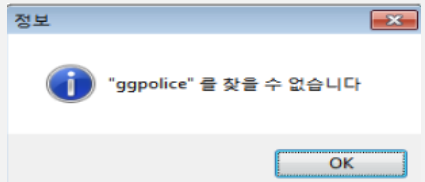
- Whale
UTF-8&sm=whl_hty&query=ggpolice - Whale
elWnd

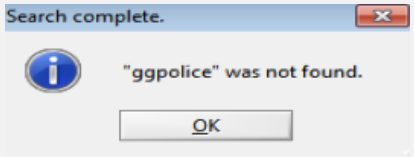


www.ggpolice.go.kr 방문 기록

메모리 덤프 파일

〈shutdown 후〉





www.ggpolice.go.kr 방문 기록

기록 없음

시크릿모드 상황분석

〈shutdown 전〉

```
loNml
STR₩Users₩sungyeon₩Downloads₩main_fl_02.jpg:Zone.Identifier
ObDi
```

```
H.L
₩Device₩HarddiskVolume2₩Users₩sungyeon₩Downloads₩main_fl_02.jpg:Zone.Identifier
Ntf0
```

Main_fl_02.jpg 다운로드 기록

메모리 덤프 파일

〈shutdown 후〉

```
HxDSetup.zi
img_award01.jpg
IMG_AW~1.JPGV
T@B
T@B
main_fl_02.jpg
T@B
T@B
MAIN_F~1.JPGV
1Fm
₩5BLm
₩5BLm
₩5BLm
winhex.
winhex.zipA
winhex.zipA
```

Main_fl_02.jpg 다운로드 기록

메모리 덤프 파일

결과정리-shutdown 전

Naver Whale

기록	일반모드	시크릿모드
검색	메모리 덤프 파일 Current Session, Current Tabs, Network Action Predictor ,Favicons, History, data_1 Pagefile.sys	기록 없음
방문 웹사이트	메모리 덤프 파일 Current Session, Current Tabs, Favicons, History, Network Action Predictor, Preference, data_1, data_2 $MFT, Pagefile.sys	메모리 덤프 파일
다운로드	메모리 덤프 파일 History, data_1 $MFT, Pagefile.sys	메모리 덤프 파일

결과정리-shutdown 후

Naver Whale

기록	일반모드	시크릿모드
검색	메모리 덤프 파일 Favicons, Network Action Predictor, Last Tabs, Last Session, History, data_1	기록 없음
방문 웹사이트	메모리 덤프 파일 Last Session, Last Tabs, Favicons, History, Network Action Predictor, Preference, cookies, data_1, data_2 $MFT, Pagefile.sys	기록 없음
다운로드	메모리 덤프 파일 History, data_1	메모리 덤프 파일

06

범죄 상황 분석

범죄 상황

어느 날 강 하류에서 친구들과 여행을 갔다던 수빈의 시신이 발견되었다.
탐정은 수빈과 함께 여행을 갔던 성연, 예린, 수경의 컴퓨터를 압수수색한다.
압수 당시 컴퓨터는 아래와 같은 상황이었다.

개인별 컴퓨터 상황

성연	수경	예린	수빈
일반모드 사용 뒤 전원 Off 후, 시크릿모드를 사용한 채로 전원 On *Naver whale 사용	일반모드와 시크릿모드를 둘 다 사용한 채로 전원 OFF *인터넷 익스플로러 사용	일반모드와 시크릿모드를 둘 다 사용한 채로 전원 On * 구글 크롬 사용	일반모드와 시크릿모드를 사용한 채로 전원 On * Firefox 사용

사망한 수빈의 브라우저

Firefox

#1

탐정은 그녀의 메일함이 비워져 있는 것을 확인한 후,
누군가 그녀의 메일함을 의도적으로 지운 것이라고 판단해 덤프 파일을 떠 보았다

*1612 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

senderName=%EA%B9%80%EC%88%98%EB%B9%88&senderAddress=&to=plko5432%40naver.com%3E
&subject=Yerin%2C%20watch%20it%20alone&body=%3Cdiv%20style%3D%22font-size%3A10pt%3B%2
Yerin%2C%20isn't%20Sukyung%20and%20Sungyeon%20too%20uncooperative%3F%20%3Cbr%3E%3C%
I%20want%20to%20take%20their%20names%20out%20of%20the%20paper.%3C%2Fp%3E%3Cp%3E
How%20about%20you%3F%3C%2Fp%3E%3Cp%3E%3Cbr%3E%3C%2Fp%3E%3C%2Fdiv%3E&rawBody=9

덤프 내용을 통해 이메일의 내용과 수신자를 알 수 있었다.

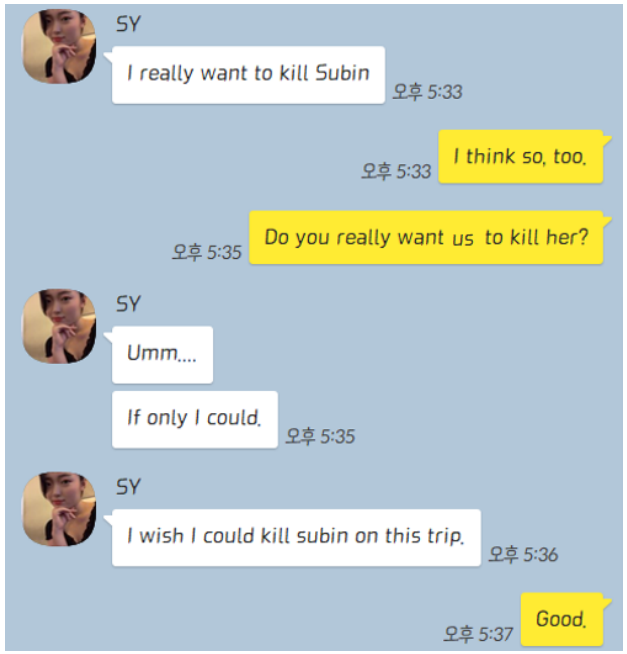
plko5432@naver.com(예린의 이메일)로
Yerin, isn't Sukyung and Sungyeon too uncooperative? I want to take their names out of the paper. How about you 라는 내용으로 메일 전송

#2

탐정은 앞서 딴 덤프 파일에서, 수빈이 누군가에게 수신한 이메일 기록을 발견했다. 이 메일의 파일의 경로를 찾아 다운로드한 파일을 확인할 수 있었다.

Look at it!!!!!! - Mozilla Firefox

file:///C:/Users/subin/Downloads/KTALKWITHSY.PNG
{"state":1,"endTime":1597104706591,"fileSize":378295}



덤프 내용을 통해 메일의 제목과 다운로드 받은 사진을 알 수 있었다.

사진은 C:/subin/Downloads/에 파일이 저장되어 있었으며
성연과 익명의 누군가가 수빈을 죽이고 싶어했다는 내용 기록

#3

수빈이 자기 자신에게 쓴 메일도 발견했다.
이 기록을 통해 탐정은 본격적으로 그녀 친구들의 컴퓨터도 조사하기 시작한다.

Eve
Eve
Io
ease investigate my friends. I never kill myself
Ntfx
VadS@
NpFRp

https://mail.naver.com/pv/write_save.jsp?orderType=toMe&attachID

덤프 내용을 통해 일부가 손상된 메일의 내용과 해당 메일이 내게 보낸 메일임을 알 수 있었다.

메일의 내용은 ese investigate my friends. I never kill myself. 로 자살이 절대 아니란 내용
OrderType=to Me로 메일 형식 기록

사망한 수빈의 브라우저

Firefox

1. 수빈은 예린에게 성연과 수경을 논문에서 제외하자는 메일을 보낸다.

2. 그리고 예린으로부터 성연과 수경이 본인을 죽이고 싶어한다는 사실을 전달받게 된다.

3. 수빈은 메일 내게쓰기 기능을 이용해 도움을 요청해 둔다.

4. 그리고 수빈은 죽게 된다.

목격자 예린의 브라우저

Chrome

#1

예린의 컴퓨터를 압수 수색한 탐정은 덤프파일을 생성한 후,
예린이 수빈과 나눈 메일의 흔적을 발견하였다.

https://mail.naver.com/#%7B%22fClass%22%3A%22read%22%2C%22oParameter%22%3A%7B%22charset%22%3A%22%
%22prevNextMail%22%3Atrue%2C%22threadMail%22%3Atrue%2C%22listScrollPosition%22%3A0%2C%22mailSN%22%3
%222656%22%2C%22previewMode%22%3A2%2C%22type%22%3A%22all%22%7D%7DYerin, watch it alone

C:₩Users₩yerin₩AppData₩Local₩Google₩Chrome₩User Data₩Default
https://nv.veta.naver.com/fxshow?su=SU10601&calp=1&nrefreshx=1
wod
tps://mail.naver.com/json/newmail/?mailSN=2660&u=plko5432

Yerin, watch it alone

보낸사람 VIP 김수빈<btsiu@naver.com>

받는사람 <plko5432@naver.com>

Yerin, isn't Sukyung and Sungyeon too uncooperative?
I want to take their names out of the paper.
How about you?

덤프파일 분석을 통해 이메일 기록을 확인할 수 있었다.

메일의 제목이 있는 위의 링크로 들어가니
Plko5432라는 아이디를 사용해 보낸 메일의 내용을 확인할 수 있었다

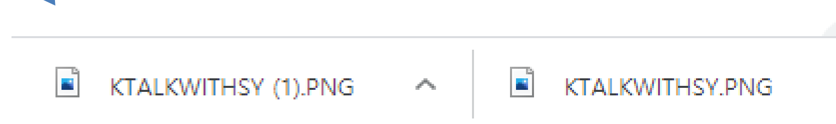
06

#2

다른 친구와의 메일 흔적을 찾기 위하여 덤프파일을 분석하던 탐정은
수경으로부터 받은 메일흔적을 발견하였다.

https://mail.naver.com/read/2659#%7B%22fClass%22%3A%22write%22%2C%22oParameter%22%3A%7B%22orderType%22%3A%22new%22%2C%22sMailList%22%3A%222659%22%7D%7D
We're angry

94109406-0331-4708-8d18-8edeb376e47aC:₩Users₩yerin₩Downloads₩KTALKWITHSY.PNGC:₩Users₩yerin₩Downloads₩KTALKWITHSY.PNG
₩Jhttps://mail.naver.com/read/2659https://mail.naver.com/read/2659https://www.naver.com/my.htmlimage/pngimage/png
https://download.mail.naver.com/file/download/each/?attachType=normal&mailSN=2659&attachIndex=2&virus=1&domain=mail.naver.com&u=plko5432



We're angry라는 제목의 링크로 들어가면 메일 내용을 확인할 수 있다.
KTALKWITHSY.PNG의 이름이 있는 메일의 아래 링크로 들어가면
예린이 다운로드 받았던 파일을 다운로드 받을 수 있다

#3

예린이 수빈에게 보낸 메일 또한 발견하였다.

<ts
x4ns
r.p
Look at it!!!!!!

https://mail.naver.com/json/newmail/?mailSN=2660&u=plko5432

senderName=%EC%95%88%EC%98%88%EB%A6%B0&senderAddress=&to=btsiu%40naver.com%3B&cc=&bcc=&subject=Look%20at%20it!!!!!!&body=%3Chtml%3E%3Chead%3E%3Cstyle%3Ep%7Bmargin-top%3A0px%3Bmargin-bottom%3A0px%3B%7D%3C%2Fstyle%3E%3C%2Fhead%3E%3Cbody%3E%3Cdiv%20style%3D%22font-size%3A10pt%3B%20font-family%3AGulim%2C%20sans-serif%3B%22%3E%3Cp%3EI'm%20so%20scared%20of%20them%20to%20talk%20about%20this...%3C%2Fp%3E%3C%2Fdiv%3E%3C%2Fbody%3E%3C%2Fhtml

Look at it이라는 제목의 메일을 수빈(btsiu@naver.com)의 메일로 보낸 것을 알 수 있다

#4

시크릿모드를 조사하던 탐정은 누군가의 블로그 주소를 발견하였고
이는 예린의 개인 블로그였다.

mR?
https://dyoerr9030.tistory.com/
G*)U

카테고리 없음

sad ending

by Y06 · 2020. 8. 13. · 수정 · 삭제

secret mod blog

Evidence mod.zip
1.58MB

블로그 주소를 통해 들어가보니 첨부파일과 함께
Sad ending이라는 제목의 게시글을 확인할 수 있었다

#5

블로그에서 첨부 파일을 다운받아 보았으나 손상되어 있는 상태였다.
이에 수상함을 느낀 경찰은 HxD Editer로 파일의 형태를 PNG로 복구시켜 보았다

Sadending.png
이 파일 형식은 지원되지 않는 것 같습니다.

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded
00000000  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  %PNG....
```

Sadending

지원되지 않는 파일 형식의 파일은 HxD로 파일 형태를 바꾸어 복구시킬 수 있다.
경찰은 사건 당시의 사진을 얻게 된다.

#6

Sad ending.png엔 수경과 성연이 수빈을 밀고 있는 모습이 정확히 포착되어 있었다.
수경과 성연에게 이에 대한 정황을 묻자 그녀들은 매우 당황하며
실수였음을 강조한다. 과연 실수였을까 고의였을까?

목격자 예린의 브라우저

Chrome

1. 예린은 수빈으로부터 성연과 수경을 논문에서 제외하자는 메일을 받게 된다.

2. 예린은 이를 성연과 수경에게 메일을 통해 전달한다.

3. 성연과 수경에게 수빈을 죽이고 싶다는 이야기를 듣고, 이 또한 수빈에게 메일을 통해 전달한다.

4. 성연과 수경이 수빈을 죽이는 장면을 목격하고, 증거 사진을 찍어 자신의 블로그에 올린다.

수빈을 죽인 수경의 브라우저

Internet Explorer

#1

탐정은 꺼져 있는 수경의 컴퓨터를 켜 아티팩트를 분석했다.
예린이 수경에게 이메일을 보낸 기록을 찾을 수 있었다.

\$MFT 4 hours ago

Name	Ext.	Size	Created	Modified	Record ch
.. = (Root directory)		8.2 KB	09-07-14d11:38:56	20-08-10d07:37:36	20-08-10d

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00306677984	88	EC	98	88	EB	A6	B0	22	2C	22	65	6D	61	69	6C	22	ˆì˜ˆë¦°",“email”
00306678000	3A	22	70	6C	6B	6F	35	34	33	32	40	6E	61	76	65	72	:"plko5432@naver
00306678016	2E	63	6F	6D	22	7D	2C	22	73	75	62	6A	65	63	74	22	.com"},"subject"
00306678032	3A	22	47	75	79	73	2C	20	68	61	76	65	20	79	6F	75	:"Guys, have you
00306678048	20	73	65	65	6E	20	74	68	69	73	3F	22	2C	22	72	65	seen this?","re
00306678064	63	65	69	76	65	64	54	69	6D	65	22	3A	31	35	39	37	ceivedTime":1597
00306678080	33	30	36	30	32	32	2C	22	73	65	6E	74	54	69	6D	65	306022,"sentTime
00306678096	22	3A	31	35	39	37	33	30	36	30	32	32	2C	22	73	69	":1597306022,"si
00306678112	7A	65	22	3A	32	31	39	32	35	2C	22	61	74	74	61	63	ze":21925,"attac
00306678128	68	43	6F	75	6E	74	22	3A	31	2C	22	69	44	6F	6D	61	hCount":1,"iDoma
00306678144	69	6E	45	6D	61	69	6C	22	3A	22	73	75	30	5F	5F	30	inEmail":"su0__0
00306678160	73	75	40	6E	61	76	65	72	2E	63	6F	6D	22	2C	22	70	su@naver.com","p

WinHex 분석을 통해 이메일 기록을 확인할 수 있다.

plko5432@naver.com(예린의 이메일)으로부터 수경(su0__0su)이 메일을 받았다.
Guys, have you seen this?라는 제목을 확인할 수 있지만, 내용은 알 수 없었다.

#2

WinHex 분석을 계속하다 성연으로부터 받은 새로운 이메일 기록을 찾았다.

\$MFT 4 hours ago

Name	Ext.	Size	Created	Modified	Record c
.. = (Root directory)		8.2 KB	09-07-14d11:38:56	20-08-10d07:37:36	20-08-10

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00306676352	84	B1	EC	97	B0	22	2C	22	65	6D	61	69	6C	22	3A	22	„±ì–°","email":"
00306676368	6C	69	7A	30	39	30	34	35	40	6E	61	76	65	72	2E	63	liz09045@naver.c
00306676384	6F	6D	22	7D	2C	22	73	75	62	6A	65	63	74	22	3A	22	om"},"subject":"
00306676400	49	26	23	33	39	3B	6D	20	73	6F	20	75	70	73	65	74	I'm so upset
00306676416	21	21	22	2C	22	72	65	63	65	69	76	65	64	54	69	6D	!!","receivedTim
00306676432	65	22	3A	31	35	39	37	33	30	36	34	33	31	2C	22	73	e":1597306431,"s
00306676448	65	6E	74	54	69	6D	65	22	3A	31	35	39	37	33	30	36	entTime":1597306
00306676464	34	33	31	2C	22	73	69	7A	65	22	3A	32	31	37	31	2C	431,"size":2171,
00306676480	22	61	74	74	61	63	68	43	6F	75	6E	74	22	3A	30	2C	"attachCount":0,
00306676496	22	69	44	6F	6D	61	69	6E	45	6D	61	69	6C	22	3A	22	"iDomainEmail":"
00306676512	73	75	30	5F	5F	30	73	75	40	6E	61	76	65	72	2E	63	su0__0su@naver.c
00306676528	6F	6D	22	2C	22	70	72	69	6F	72	69	74	79	22	3A	33	om","priority":3

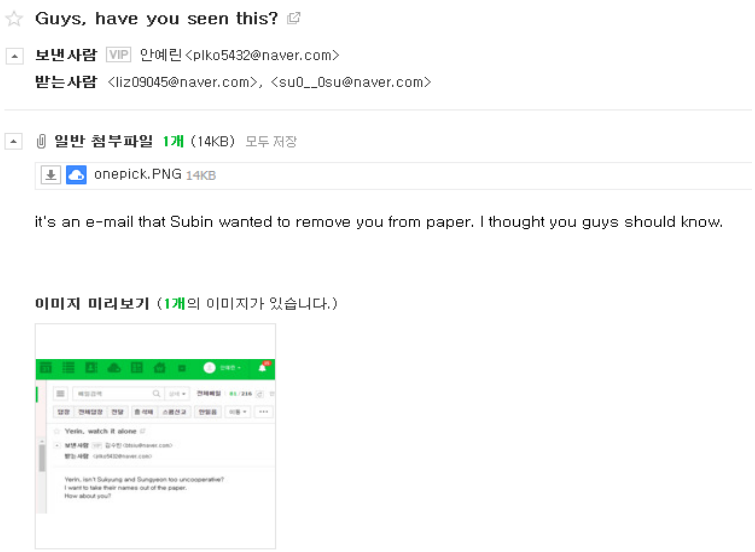
liz09045@naver.com (성연의 이메일)로부터 수경이 메일이 받았음을 알 수 있다.
이번 기록 역시 제목인 I'm so upset!!를 확인할 수 있지만, 내용을 알 수 없었다.

#3

탐정은 이메일에 대한 자세한 정보를 알기 위해
Internet Explorer의 WebCacheV01.dat 파일 정보를 분석해봤다.

History(M)_Recovered | History(L)_Recovered | MSHist012020081320200814(M)_... | Content(L)_Recovered

AccessedTime	PostCheckTime	Url	WebPageInfo
2020-08-10 14:...	0	Visited: sue@http://go.microsoft.com/fwlink/?LinkId=2294...	
2020-08-10 16:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-13 17:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 16:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	MSN - 뉴스, 핫메일, Hotmail, Skype, 아웃룩 메일, 윈드...
2020-08-10 16:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	MSN - 뉴스, 핫메일, Hotmail, Skype, 아웃룩 메일, 윈드...
2020-08-10 17:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 18:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 18:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 17:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	MSN - 뉴스, 핫메일, Hotmail, Skype, 아웃룩 메일, 윈드...
2020-08-10 17:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	MSN - 뉴스, 핫메일, Hotmail, Skype, 아웃룩 메일, 윈드...
2020-08-10 18:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 19:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 19:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 19:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 19:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 19:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 19:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 19:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 19:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 19:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 19:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 19:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	//static-global-s-msn-com.akamaized.net/hp-eas/sc/1f/08...
2020-08-10 18:...	0	Visited: sue@http://www.msn.com/ko-kr/?ocid=iehp&pc=...	MSN - 뉴스, 핫메일, Hotmail, Skype, 아웃룩 메일, 윈드...
2020-08-13 17:...	0	Visited: sue@https://www.bing.com/search?q=naver.com...	naver.com - Bing
2020-08-13 17:...	0	Visited: sue@https://www.bing.com/search?q=naver.com...	naver.com - Bing
2020-08-13 17:...	0	Visited: sue@https://www.naver.com/	NAVER
2020-08-13 20:...	0	Visited: sue@https://www.naver.com/	NAVER
2020-08-13 17:...	0	Visited: sue@https://www.naver.com/	NAVER
2020-08-13 17:...	0	Visited: sue@https://nid.naver.com/nidlogin.login?mode=f...	네이버 : 로그인
2020-08-13 17:...	0	Visited: sue@https://nid.naver.com/nidlogin.login?mode=f...	네이버 : 로그인
2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/read/103	네이버 메일



onepick.PNG

예린이 보낸 메일의 상세 내용을 확인할 수 있었다.

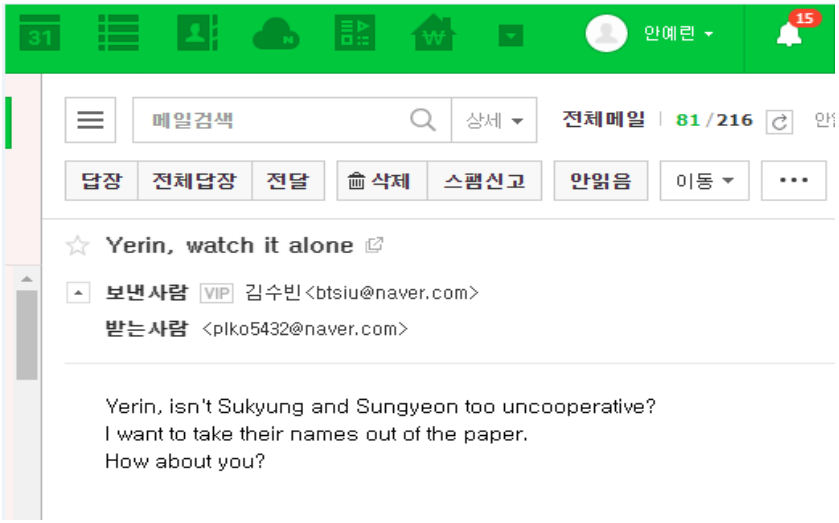
수경이 메일을 확인했다는 기록을 History 파일에서 찾을 수 있었고,
해당 URL을 따라가면 예린이 보낸 메일을 볼 수 있다.

#4

예린에게서 보낸 메일에서 받은 첨부파일 기록도 확인할 수 있다.
파일을 저장한 경로와 파일 이름까지도 확인할 수 있다.

History(M)_Recovered | History(L)_Recovered | MSHist012020081320200814(M)_... | Content(L)_Recovered

AccessedTime	PostCheckTime	Url	WebPageInfo
2020-08-13 17:...	0	Visited: sue@file:///C:/Users/sue/Downloads/onepick.PNG	



History파일에서 다운로드 받은 사진 파일을 확인할 수 있다.
파일 경로 : C://sue/Downloads/onepick.PNG 를 찾아가면 onepick.PNG을 찾을 수 있다.

#5

수경이 일반 모드에서 검색한 검색 기록을 찾을 수 있었다.

Table

No.	Table Name	Count
11	Content(M)_Recovered	23
12	History(M)_Recovered	90
13	feedplat(M)_Recovered	1
14	iecompat(M)_Recovered	6970
15	iecompatua(M)_Recovered	23
16	History(L)_Recovered	278
17	Cookies(M)_Recovered	2
27	Content(L)_Recovered	1831
30	Cookies(L)_Recovered	71
32	DOMStore(L)_Recovered	13
33	MSHist012020081020200811(M)_Recovered	38
37	iedownload(M)_Recovered	3
42	MSHist012020081320200814(M)_Recovered	20

History(M)_Recovered | History(L)_Recovered | MSHist012020081320200814(M)_... | Content(L)_Recovered

edTime	AccessedTime	PostCheckTime	Url	WebPageInfo
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://search.naver.com/search.naver	
08-13 1...	2020-08-13 17:...	0	Visited: sue@https://search.naver.com/search.naver?sm=...	Cliff : 네이버 통합검색
08-13 1...	2020-08-13 17:...	0	Visited: sue@https://ad.naver.com/bxshow?su=SU10415&...	
08-13 1...	2020-08-13 17:...	0	Visited: sue@https://dict.naver.com/search.nhn?query=Cli...	'Cliff'의 검색결과 : 네이버 사전
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://cc.naver.com/cc?a=gnb.mail&r=1&i=...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=0&p...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/	받은메일함(12) : 네이버 메일
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=0&p...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=0&p...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=0&p...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=all&...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=all&...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=0&p...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=0&p...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=0&p...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=all&...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=all&...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=all&...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=0&p...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/read.jsp?mailsn=1...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/write.jsp?orderTy...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/write_save.jsp?or...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/write_save.jsp?or...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/read.jsp?mailsn=1...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=0&p...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/read.jsp?mailsn=1...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/write.jsp?orderTy...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=all&...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/write_save.jsp?or...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/sendresult.jsp?att...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://mail.naver.com/pv/list.jsp?folder=0&p...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://cc.naver.com/cc?a=gnb.naver&r=&i=...	
08-13 2...	2020-08-13 20:...	0	Visited: sue@https://search.naver.com/search.naver?sm=...	Accidental accident : 네이버 통합검색

Cliff(절벽), Accidental accident(우발적 사고)를 검색한 기록이
History파일에 남아 있다.

#6

시크릿 모드에서 검색한 내용도 찾을 수 있었다.
이 기록을 통해 수경은 우발적 사고를 계획했다는 정황을 확인할 수 있다.

Content(L)_Recovered

	EntryId	FileSize	Type	AccessCount	SyncTime	CreationTime
	1477	129	[Normal][PrivateBrowsing]	1	2020-08-13 18:12:34	2020-08-13 18:12:34
	1477	129	[Normal][PrivateBrowsing]	1	2020-08-13 18:12:34	2020-08-13 18:12:34

Url
https://ac.search.naver.com/nx/ac?_callback=window.__jindo_callback._$3361_10&q=murder sente&q_enc=UTF-8&st=100&frm=nv&r_form...
https://ac.search.naver.com/nx/ac?_callback=window.__jindo_callback._$3361_10&q=murder sente&q_enc=UTF-8&st=100&frm=nv&r_form...
https://ac.search.naver.com/nx/ac?_callback=window.__jindo_callback._$3361_12&q=murder sentenc&q_enc=UTF-8&st=100&frm=nv&r_for...
https://ac.search.naver.com/nx/ac?_callback=window.__jindo_callback._$3361_13&q=murder sentence&q_enc=UTF-8&st=100&frm=nv&r_f...
https://ac.search.naver.com/nx/ac?_callback=window.__jindo_callback._$3361_13&q=murder sentence&q_enc=UTF-8&st=100&frm=nv&r_f...
https://ac.search.naver.com/nx/ac?_callback=window.__jindo_callback._$3361_11&q=murder senten&q_enc=UTF-8&st=100&frm=nv&r_for...

Private Browsing 이라는 문구를 통해 시크릿 모드에서의 기록임을 알 수 있다.
Murder sentence (살인 형량)을 검색한 기록을 찾을 수 있다.

수빈을 죽인 수경의 브라우저

Internet Explorer

1. 수경은 예린으로부터 받은 메일을 보고 수빈을 죽이고자 한다.

2. 성연과의 메일을 통해 살인 계획을 세우고,
살인에 관한 얘기를 예린에게 메일을 통해 전달한다.

3. 살인 관련한 검색을 통해 정보를 수집한다.

4. 성연과 함께 수빈을 절벽에서 떨어트려 살인을 저지른다.

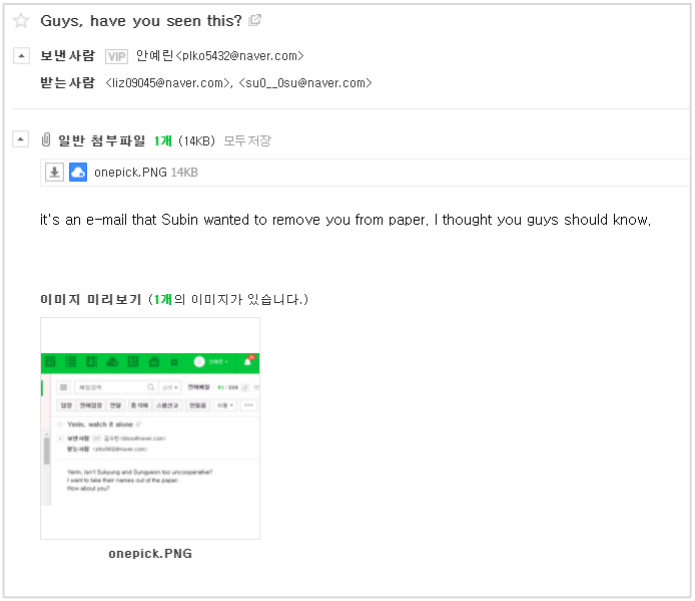
수빈을 죽인 공범 성연의 브라우저

Naver Whale

#1

탐정은 성연이 컴퓨터로 어떤 활동을 했는지 찾기 위해 덤프파일을 생성했다.
덤프파일을 통해 성연의 이메일 기록을 찾을 수 있었다.

https://mail.naver.com/read/image/?
mailSN=3118&attachIndex=2&contentType=image/png&offset=2541&size=19326&mimeSN=15'
306022.467674.17861.42752&org=1&u=liz09045image (520
357)
https://mail.naver.com/read/3117#%7B%22fClass%22%3A%22read%22%2C%22oParameter
%22%3A%7B%22charset%22%3A%22%22%2C%22prevNextMail%22%3Atrue%2C
%22threadMail%22%3Atrue%2C%22listScrollPosition%22%3A0%2C%22mailSN%22%3A
%223118%22%2C%22previewMode%22%3A2%7D%7DGuys, have you seen this?(379)
https://mail.naver.com/read/3117#%7B%22fClass%22%3A%22list%22%2C%22oParameter
%22%3A%7B%22page%22%3A1%2C%22sortField%22%3A1%2C%22sortType%22%3A0%2C
%22folderSN%22%3A%220%22%2C%22type%22%3A%22%22%2C%22isUnread%22%3Afalse
%7D%7D



방문 기록 url 들을 살펴보면서 각각 링크로 들어가 보았더니,
예린으로부터 얻은 이메일을 확인할 수 있었다. (일반모드)

#2

덤프파일에서 수경으로부터 받은 이메일 내용을 확인할 수 있다.
이는 일반모드에서 확인한 메일이었다.

3bbb489d-1ee0-4f8b-a7db-2f9c38859e42C:₩Users₩sungyeon₩Downloads₩onepick.PNGC:
₩Users₩sungyeon₩Downloads₩onepick.PNG
7(7(
T#₩
9https://mail.naver.com/read/3117https://mail.naver.com/read/3117#%7B%22fClass%22%3A
%22read%22%2C%22oParameter%22%3A%7B%22charset%22%3A%22%22%2C
%22prevNextMail%22%3Atrue%2C%22threadMail%22%3Atrue%2C%22listScrollPosition
%22%3A0%2C%22mailSN%22%3A%223118%22%2C%22previewMode%22%3A2%7D
%7Dhttps://mail.naver.com/read/3117#%7B%22fClass%22%3A%22list%22%2C%22oParameter
%22%3A%7B%22page%22%3A1%2C%22sortField%22%3A1%2C%22sortType%22%3A0%2C
%22folderSN%22%3A%220%22%2C%22type%22%3A%22%22%2C%22isUnread%22%3Afalse
%7D%7Dimage/pngimage/png
https://mail.naver.com/read/3121#%7B%22fClass%22%3A%22read%22%2C%22oParameter
%22%3A%7B%22charset%22%3A%22%22%2C%22prevNextMail%22%3Atrue%2C
%22threadMail%22%3Atrue%2C%22listScrollPosition%22%3A0%2C%22mailSN%22%3A
%223121%22%2C%22previewMode%22%3A2%7D%7DI'M SOOOOO ANGRY!!
https://mail.naver.com/read/3121#%7B%22fClass%22%3A%22list%22%2C%22oParameter
%22%3A%7B%22page%22%3A1%2C%22sortField%22%3A1%2C%22sortType%22%3A0%2C
%22folderSN%22%3A%221%22%2C%22type%22%3A%22%22%2C%22isUnread%22%3Afalse
%7D%7D

사건의 발단은 수빈이 성연과 수경을 논문에서 이름을 제외할 것이라고
예린에게 얘기했던 것이 범행 동기가 되었다는 것을 확인할 수 있다.

#3

성연은 먼저 수경에게 수빈을 죽이자며 시크릿모드로 메일을 보낸다

Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.106 Whale/2.8.105.22 Safari/537.36
Content-Type
application/x-www-form-urlencoded; charset=UTF-8
Accept
/
senderName=%EA%B9%80%EC%84%B1%EC%97%B0&senderAddress=&to=%22%EC%84%9C
%EC%9A%B8%EC%97%AC%EB%8C%80%20%EC%A0%95%EB%B3%B419%20%EC%A1%B0%EC
%88%98%EA%B2%BD%22%3Csu0__0su%40naver.com%3E%3B&cc=&bcc=&subject=Let's
%20bury%20Subin%20here.&body=%3Cdiv%20style%3D%22font-size%3A10pt%3B%20font-
family%3AGulim%2C%20sans-serif%3B%22%3E%3Cp%3EYou%20kill%20her%2C%20and
%20then%20I%20will%20bury%20at%20Gangnueng%20Cliff.%3C%2Fp%3E%3C%2Fdiv
%3E&rawBody=%3Cp%3EYou%20kill%20her%2C%20and%20then%20I%20will%20bury%20at
%20Gangnueng%20Cliff.%3C%2Fp
%3E&contentType=html&sendSeparately=false&saveSentBox=true&type=draft&fromMe=0&atta
chID=nlY-KAgZKAUTKqE-BqKwWz0PKAvmFAETKxUqKx2-KAg-
Fov.&reserveDate=&reserveGMT=&reserveTime=&calendarVal=&autoSaveMailSN=3126&attach
Count=0&attachSize=0&bigfile=0&sessionID=&seqNums=&priority=0&ndriveFileInfos=&threadI
d=&savedType=new&savedLists=&marked=false&u=liz09045
WW
XIV

su0__0su@naver.com 으로
Let's bury subin here … you kill her and then I will bury her at Gangnueng Cliff…
라는 내용의 메일을 전송했음이 기록되어 있다.

#4

성연은 다시 수경에게 내일 강릉여행에서 수빈을 죽이고,
묻어버리자는 계획을 시크릿모드를 통해 메일로 보낸다.

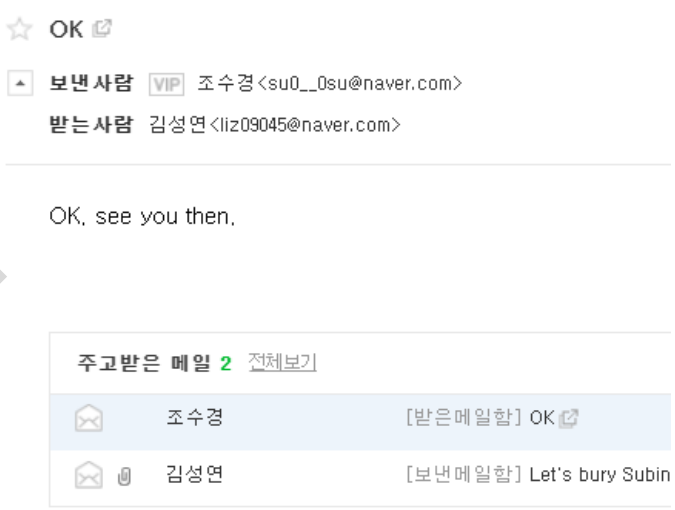
Chrome/83.0.4103.106 Whale/2.8.105.22 Safari/537.36
Content-Type
application/x-www-form-urlencoded; charset=UTF-8
Accept
/
senderName=%EA%B9%80%EC%84%B1%EC%97%B0&senderAddress=&to=%22%EC%84%9C
%EC%9A%B8%EC%97%AC%EB%8C%80%20%EC%A0%95%EB%B3%B419%20%EC%A1%B0%EC
%88%98%EA%B2%BD%22%3Csu0__0su%40naver.com%3E%3B&cc=&bcc=&subject=R%20U
%20READY%3F&body=%3Cdiv%20style%3D%22font-size%3A10pt%3B%20font-family
%3AGulim%2C%20sans-serif%3B%22%3E%3Cp%3ETomorrow%20is%20the%20day%20that
%20we%20have%20to%20kill%20subin.%3C%2Fp%3E%3Cp%3E%3Cbr%3E%3C%2Fp%3E%3C
%2Fdiv%3E&rawBody=%3Cp%3ETomorrow%20is%20the%20day%20that%20we%20have
%20to%20kill%20subin.%3C%2Fp%3E%3Cp%3E%26nbsp%3B%3C%2Fp
%3E&contentType=html&sendSeparately=false&saveSentBox=true&type=draft&fromMe=0&atta
chID=nlY-KAgZKAUTKqE-BqKwWz0PKAvmFAETaAtwKqu-
KxEXKxMl&reserveDate=&reserveGMT=&reserveTime=&calendarVal=&autoSaveMailSN=3124&a
ttachCount=0&attachSize=0&bigfile=0&sessionID=&seqNums=&priority=0&ndriveFileInfos=&thr
eadId=&savedType=new&savedLists=&marked=false&u=liz09045
L=.
U
@5

su0__0su@naver.com 으로
R U READY…Tomorrow is the day that we have to kill subin…
라는 내용의 메일을 전송했음이 기록되어 있다.

#5

성연이 수경으로부터 살인에 대해 동의하는 답장메일을 보냈음을 알 수 있다.

E&0
s,-
POST
https://mail.naver.com/json/read/?charset=&prevNextMail=true&threadMail=true&listScrollPosition=0&mailSN=3128&previewMode=2&u=liz09045
https
naver.com
https
mail.naver.com
https://mail.naver.com/read/3128
charset
utf-8
X-Requested-With
XMLHttpRequest
If-Modified-Since
Thu, 1 Jan 1970 00:00:00 GMT
User-Agent
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.106 Whale/2.8.105.22 Safari/537.36
Content-Type



덤프파일에 있는 url에 들어가면 수경의 답장을 확인할 수 있다.
이를 통해 수경의 아티팩트 분석에서 자세히 알지 못했던 다른 메일 기록들을
성연의 덤프파일에서 확인할 수 있었다.

#6

그리고 성연은 범행에 관련한 내용에 대해 인터넷 검색을 진행했음이 기록되어있다.

IEND
ttps://search.naver.com/search.naver?sm=tab_hty.top&where=nexearch&query=killing
+skill&oquery=gangneung+cliff&tqi=UzRFowprvN8ssk3Yd2Nsssssh0-096890
fftBff~Af
Whale
s&sm=tab_jum&query=statue+of+limitation - Whale
query=killing+skill&tqi=UzRovlp0YiRssUywZr0ssssstAl-124537 - Whale
MSCTFIME Composition

265402&q=abandonment+of+the
+body&ie=utf8&rev=1&ssc=tab.nx.all&f=nexearch&w=nexearch&s=9G9zmJNt
%2BoijZzpsi1MtAlwu&time=1597306915312&bt=6&a=sta.naver&r=&i=&u=https%3A%2F
%2Fwww.naver.com%2FNAVER
https://search.naver.com/search.naver?
sm=tab_hty.top&where=nexearch&query=abandonment+of+the
+body&oquery=abandonmnet+of+the+body&tqi=Uzg35lprvOsssdmX07wsssssHw-
220676abandonment of the body :
https://search.naver.com/search.naver?sm=top_hty&fbm=1&ie=utf8&query=abandonmnet+of
+the+bodyabandonmnet of the body :

Abandonment of the body (시신유기), gangnueng cliff(강릉 절벽), killing skill(살인기술)
에 대한 검색기록이 남아있다.
일반모드와 시크릿 모드에서 검색했던 기록들이 모두 남아있다.

#7

또한 성연이 범행에 관련한 내용에 대해 블로그에 접속했던 기록도 확인할 수 있다.

tps://blog.naver.com/dewygirl97?Redirect=Log&logNo=221881173479
p=UzRoUlp0JXVsshXo5Glsssssscl-348587&q=statue+of
+limitation&ie=utf8&rev=1&ssc=tab.nx.all&f=nexearch&w=nexearch&s=WSDEwRz36E7vedDJeY
mWUWKa&time=1597317253327&bt=18&a=blg_1st*i.tit&r=1&i=90000003_0000000000000033A92
605E7&u=https%3A%2F%2Fblog.naver.com%2Fdewygirl97%3FRedirect%3DLog%26logNo
%3D221881173479&cr=1

Statue of limitation(공소시효)에 관련한 블로그에 접속했던 기록이 확인가능하고,
시크릿모드로 접속했던 블로그임에도 불구하고 기록이 남아있다.
해당 링크로 들어가면 블로그의 글도 확인이 가능하다.

#8

탐정은 성연이 시크릿모드를 통해
공소시효와 관련된 다운로드를 한 기록을 확인할 수 있었다.

```
GET
https://www.kci.go.kr/kciportal/co/download/popup/poDownload.kci?
storFileBean.orteFileId=KCI_FI001362575
https
kci.go.kr
https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?
sereArticleSearchBean.artiId=ART001362575
HTTP/1.1 302 Found
Date: Thu, 13 Aug 2020 11:51:45 GMT
Server: IBM_HTTP_Server
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline' https://fonts.googleapis.com; font-src 'self' https://fonts.gstatic.com; frame-src 'self'
https://translate.kci.go.kr https://ernd.nrf.re.kr https://www.jams.or.kr; img-src 'self' 'unsafe-inline'
X-Content-Type-Options: nosniff
Location: https://www.kci.go.kr/kciportal/co/download/popup/poDownload.kci?
storFileBean.orteFileId=KCI_FI001362575
Content-Length: 0
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Keep-Alive: timeout=10, max=94
Connection: Keep-Alive
Content-Type: text/plain
Content-Language: ko-KR
text/plain
```

```
type
value
C:₩Users₩sungyeon₩Downloads₩KCI_FI001362575.pdf
rdownload
type
```

다운로드를 받은 사이트, 파일이 저장된 위치 등을 확인할 수 있었다.
이를 통해, 성연이 계획적인 범행을 저질렀다는 정황을 파악할 수 있다.

수빈을 죽인 공범 성연의 브라우저

Naver Whale

※ 압수 당시, 성연의 PC는 시크릿모드 브라우저가 켜진 채로 있었고,
나머지 기록들(일반모드)은 모두 이전에 활동한 뒤 한번 이상 PC 종료가 있었다

1. 성연은 예린으로부터 받은 메일을 보고
수경에게 수빈을 죽이자고 제안한다.

2. 수경과의 메일을 통해 살인 계획을 세우고,
살인 관련한 검색을 통해 정보를 수집한다.

4. 수경과 함께 수빈을 절벽에서 떨어트려 살인을 저지른다.

.

탐정은 그렇게 수경과 성연이 수빈을 고의로 죽였다는 정황들을 파악했다.
이를 성연과 수경, 그리고 예린에게 알리고
결국 성연과 수경은 자백을 하게 된다.

THANK YOU

발표자 아티fact체크!